Militärische Cyber-Operationen: Nutzen, Limitierungen und Lehren für Deutschland

Schulze, Matthias

SWP

SWP-Studie

Matthias Schulze

Militärische Cyber-Operationen

Nutzen, Limitierungen und Lehren für Deutschland

Stiftung Wissenschaft und Politik
Deutsches Institut für
Internationale Politik und Sicherheit

SWP-Studie 15
August 2020, Berlin

- Offensive Militärische Cyber-Operationen (OMCO) sind — anders als in populären Darstellungen oft behauptet — keine Allzweckwaffe. Sie unterliegen zahlreichen strategischen, operativen und taktischen Begrenzungen, die sie für bestimmte Einsatzszenarien ungeeignet erscheinen lassen.
- Deutschland sollte auch in Zukunft daran festhalten, keine strategischen OMCO zu planen und zu entwickeln. Der strategische Einsatz von OMCO ist operativ zu aufwendig, extrem risikobehaftet und zudem der globalen Sicherheit des Cyber- und Informationsraums unzuträglich.
- Sehr limitierte und überschaubare Cyber-Operationen zur sequenziellen Begleitung von Kampfeinsätzen können bei hochtechnisierten Gegnern sinnvoll sein. Der größte Nutzen von OMCO liegt in ihrer Spionagefunktion und weniger in disruptiven, zerstörerischen militärischen Effekten.
- Für das typische Einsatzprofil der Bundeswehr, nämlich Konfliktmanagement in wenig digitalisierten Regionen mit schwacher Staatlichkeit, dürften militärische Cyber-Operationen nur in wenigen Fällen einen militärischen Nutzen haben.
- Um effektiv zu sein, müssen OMCO auf Ziele exakt zugeschnitten sein. Bei einem OMCO-Einsatz zur Landesverteidigung müssen daher schon im Vorfeld und noch zu Friedenszeiten Zielinformationen beim potentiellen Gegner erhoben worden sein — mittels offensiver Cyber-Spionage in fremden Netzen. Diese Präemptionslogik erzeugt aber ein Sicherheitsdilemma bei potentiellen Gegnern und kann destabilisierend wirken.

SWP-Studie

Matthias Schulze

Militärische Cyber-Operationen

Nutzen, Limitierungen und Lehren für Deutschland

Stiftung Wissenschaft und Politik
Deutsches Institut für
Internationale Politik und Sicherheit

SWP-Studie 15
August 2020, Berlin

SWP-Studien unterliegen einem Verfahren der Begutachtung durch Fachkolleginnen und -kollegen und durch die Institutsleitung *(peer review)*, sie werden zudem einem Lektorat unterzogen. Weitere Informationen zur Qualitätssicherung der SWP finden Sie auf der SWP-Website unter https://www.swp-berlin.org/ueber-uns/qualitaetssicherung/. SWP-Studien geben die Auffassung der Autoren und Autorinnen wieder.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3—4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-200
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1611-6372
doi: 10.18449/2020S15

Inhalt

5 Problemstellung und Schlussfolgerungen

7 Einführung

9 Militärische Cyber-Operationen

13 Die Bundeswehr im Cyber- und Informationsraum
15 Genese und Funktion offensiver Cyber-Fähigkeiten in den strategischen Dokumenten der Bundeswehr

19 Strategisch, operativ, taktisch: Typen von OMCO am Beispiel anderer Länder
19 Strategische OMCO
22 Operative OMCO
26 Taktische OMCO
28 Zusammenfassung und Typologie verschiedener OMCO

32 Sinnvolle Einsatzszenarien für offensive Bundeswehr-Cyber-Operationen
34 ISR-Operationen
35 InfoOps
36 Begrenzte DoS-OMCO zur Begleitung von Kampfeinsätzen
36 Szenario: Verteidigungsfall

39 Ergebnisse und Ausblick

40 Abkürzungen

Dr. Matthias Schulze ist stellvertretender Leiter der Forschungsgruppe Sicherheitspolitik

Militärische Cyber-Operationen. Nutzen, Limitierungen und Lehren für Deutschland

Cyber-Operationen in fremden Netzen gelten in vielen Staaten als »perfekte Waffe« bzw. »Allzweckschwert«. Denn mit ihnen lassen sich eine Reihe unterschiedlicher Effekte erzielen. Cyber-Operationen können temporäre Störungen (Disruptionen) auslösen, Daten, Systeme oder gar angeschlossene cyber-physische Systeme zerstören und zur Informationsbeschaffung genutzt werden. Daraus ergeben sich in der Theorie flexible Verwendungsmöglichkeiten: von der Beeinflussung fremder Gesellschaften über Spionage, Sabotage bis hin sogar zum »Ausschalten« ganzer Länder. Allerdings ist nicht alles, was theoretisch möglich ist, auch praktisch unter den gegebenen Rahmenbedingungen durchführbar bzw. sicherheitspolitisch sinnvoll. Analysiert man die Nutzung von Cyber-Operationen in militärischen Konflikten empirisch, stellt man fest, dass es eine große Bandbreite von verschiedenen Typen offensiver militärischer Cyber-Operationen (OMCO) gibt. Die verfügbaren Werkzeuge haben einerseits das Potential, strategische, operative und taktische Vorteile zu verschaffen, andererseits unterliegen sie aber auch zahlreichen Beschränkungen bzw. bergen sie zum Teil enorme Risiken, die sie in vielen Einsatzkontexten als ungeeignetes militärisches Mittel erscheinen lassen. Insofern stellt sich die Forschungsfrage, welche Arten von militärischen Cyber-Operationen für Deutschland vorbildhaft für eigene Bundeswehreinsätze sein können und welche operativen, technischen und rechtlichen Hindernisse es dabei gibt.

Strategische Cyber-Operationen sind jene, die auf eine Beeinflussung anderer Staaten in Friedenszeiten abzielen, ohne dabei konventionelle Streitkräfte einzusetzen. Ein Land dauerhaft digital zu stören ist ein hochkomplexes Unternehmen, erfordert viel Personal und birgt enorme Kollateral- und Eskalationsrisiken. Strategische Angriffe, egal ob konventionell oder digital, führen nur in wenigen Fällen zu politischen Konzessionen und sind daher meist militärisch wenig sinnvoll. Deshalb dürften solche Cyber-Operationen für Deutschland wegen der Begrenztheit der Ressourcen, sicherheitspolitischer Interessen und verfassungsrechtlicher Hürden nicht in Frage kommen.

Cyber-Angriffe in operativen Kontexten, also offensive Handlungen im virtuellen Raum, die im Verbund mit konventionellen Fähigkeiten bzw. Streitkräften ausgeführt werden, mögen in der Frühphase von bewaffneten Konflikten sinnvoll sein. Der größte Nutzen liegt allerdings nicht in ihrer militärischen, sondern in ihrer nachrichtendienstlichen Funktion und in der Begleitung von Informationsoperationen. Bedingt geeignet sind disruptive OMCO zur Flankierung von Kampfeinsätzen, zum Beispiel das Ausschalten von Radarsystemen oder militärischer Kommunikation. Allerdings ist die parallele Nutzung von Cyber- und konventionellen Fähigkeiten während länger andauernder Konflikte schwer zu synchronisieren. Jenseits psychologischer Effekte und von Beiträgen zur Aufklärung ist ihr militärischer Nutzen daher in den meisten empirisch-beobachtbaren Konflikten bisher begrenzt, insbesondere wenn asymmetrische, resiliente oder wenig digitalisierte Gegner bekämpft werden sollen. Allerdings kann sich das mit zunehmender Digitalisierung ändern.

Der taktische Einsatz von offensiven Cyber-Fähigkeiten zur Unterstützung von Soldaten in Gefechtskontexten, etwa bei einem Auslandseinsatz, wird dadurch erschwert, dass Schadsoftware, die für jeden Fall maßgeschneidert sein muss, kein einfach standardisierbares Werkzeug ist. Zudem stimmt die Geografie des konventionellen Einsatzorts nur selten mit der globalen Natur des Cyber- und Informationsraums überein. Daraus ergeben sich Kollateral- und Eskalationsrisiken. Für zahlreiche traditionelle Einsatzaufgaben der Bundeswehr (Logistik, humanitäre Hilfe und Versorgung, Transport und Evakuierung, Schutzaufgaben, Ausbildung und Beratung) eignen sich Cyber-Operationen daher kaum.

In einer Situation der Landesverteidigung könnten gegnerische Waffensysteme deaktiviert werden, da diese komplex und aufgrund ihrer Vernetzung und Softwareschwachstellen verwundbar sind. Allerdings impliziert die Vorbereitung solcher Cyber-Angriffe zur Verteidigung offensive Cyber-Spionageoperationen in Friedenszeiten, die potentiell das friedliche Zusammenleben der Völker gefährden.

Deshalb sollte Deutschland eine öffentliche strategische Diskussion darüber führen, welche Typen von OMCO man selbst durchführen will. Nicht alle Varianten von OMCO liegen im strategischen Interesse der Bundesrepublik, mit ihrem eher defensiven und humanitären Verständnis von Sicherheitspolitik. Im Zuge der Debatte sollte insbesondere thematisiert werden, wie sich Cyber-Operationen sinnvoll in die deutsche Außen und Sicherheitspolitik integrieren lassen, etwa für Aufgaben des Konfliktmanagements. Dieses Feld ist bisher in der Forschung und politischen Praxis komplett unterbelichtet. Dies zu ändern erfordert aber einen transparenteren und offeneren Umgang mit dem Thema und eine Abkehr von der bisherigen Politik der Geheimhaltung. Auch dürften nicht alle Arten von OMCO operativ und rechtlich durchführbar sein.

Daher braucht es eine offenere Diskussion über die teilweise sehr unterschiedlichen rechtlichen Rahmenbedingungen von Cyber-Operationen. Die Studie liefert eine Typologie verschiedener OMCO, um die politische und rechtswissenschaftliche Debatte voranzubringen. Seit 2016 konzentrieren sich die Beiträge zu dieser Thematik vor allem auf die Frage, ob das Grundgesetz den Einsatz der Bundeswehr im Cyber- und Informationsraum generell erlaubt. Die relevantere Frage indes ist, welche Typen von Cyber-Operation zum Beispiel einen Parlamentsvorbehalt benötigen und welche nicht.

Einführung

Mit dem *Weißbuch* von 2016 und der Schaffung des Kommandos Cyber- und Informationsraum (KdoCIR) hat das Bundesverteidigungsministerium (BMVg) den Grundstein dafür gelegt, dass sich die Bundeswehr an der gesamtstaatlichen Cyber-Sicherheitspolitik beteiligt. Jenseits defensiver Maßnahmen zum Schutz der eigenen Netzwerke, zu denen sie zuvor schon berechtigt war, soll die Bundeswehr nun erstmals aktiv und offensiv auf Netzwerke anderer Länder einwirken dürfen. In Deutschland haben allerdings das Innenministerium und zivile Behörden die Federführung in der Cyber-Sicherheit bzw. bei der Gefahrenabwehr, weshalb die Bundeswehr nur in bestimmten Fällen an der gesamtstaatlichen Cyber-Verteidigung mitwirken kann.[1] Insbesondere in Auslandseinsätzen sollen eigene Cyber-Angriffe der Bundeswehr eine größere Rolle spielen, da sie das »Spektrum militärischer Handlungsoptionen erweitern«.[2] In politischen Diskursen werden offensive Cyber-Fähigkeiten gerne als »perfekte Waffe« oder als »Allzweckschwert« (»all-purpose sword«) dargestellt, die eine sinnvolle Ergänzung für zahlreiche Aspekte militärischer Operationen sein können.[3] Cyber-Konflikte folgen allerdings eher der Logik von Geheimdienstrivalitäten als der bewaffneter militärischer Konflikte.[4] Das heißt, dass Cyber-Angriffe besser für Spionage und kriminelle Handlungen bzw. Aktivitäten unterhalb der Schwelle bewaffneter Konflikte geeignet sind als für das militärische Niederringen eines Gegners. Deswegen ist auch die militärische Nutzung von Cyber-Fähigkeiten in den meisten Staaten Neuland.

Im deutschen Cyber-Sicherheitsdiskurs werden diese Eigenheiten offensiver militärischer Cyber-Operationen (OMCO) kaum offen diskutiert. Die Diskussion dreht sich bisher vorwiegend um die zivile Nutzung von Cyber-Angriffen im Rahmen der aktiven Cyber-Abwehr, das heißt als Reaktion auf fremde Cyber-Attacken (sog. »Hackback«). Eine zentrale Frage dabei ist, welcher Akteur, von den Bundes- oder Länderpolizeien bis zu den Nachrichtendiensten, diese reaktiven, defensiven Cyber-Angriffe durchführen soll. Die militärische Seite indes ist weitgehend unterbelichtet. Es herrscht Unklarheit darüber, welche grundsätzlichen Ziele Deutschland mit eigenen OMCO verfolgt und wie sich diese strategisch in die deutsche Sicherheitspolitik einbetten lassen.[5] Auch die zentralen strategischen Dokumente wie das *Weißbuch* und die *Konzeption der Bundeswehr* von 2018 geben auf die Frage, inwiefern Cyber-Operationen ein sinnvolles Mittel für Deutschlands Außen- und Sicherheitspolitik sein können, keine stichhaltige Antwort. Es ist unklar, ob militärische Cyber-Fähigkeiten zum spezifischen Profil der Bundeswehr, etwa beim internationalen Konfliktmanagement, passen oder tatsächlich zur Landesverteidigung beitragen können. Es gibt auch keine Diskussion darüber, welche *Arten* von Cyber-Operationen von Deutschland zu erwarten sind. Diesbezügliche parlamentarische Anfragen werden in der Regel mit dem Verweis auf den Geheimschutz nicht beantwortet.[6]

Allerdings gibt es eine riesige Bandbreite von Möglichkeiten für den Einsatz von OMCO. Diese reichen von strategischer Informationsbeeinflussung in Friedenszeiten nach russischem Vorbild über das strategische »Ausschalten« gesamter Nationen bis hin zu

1 Bundesregierung, *Weißbuch. Zur Sicherheitspolitik und zur Zukunft der Bundeswehr*, Berlin 2016, S. 102, <https://bit.ly/2Zpz8hz> (wenn nicht anders gekennzeichnet, wurde auf sämtliche Internetquellen, auf die in dieser Studie verwiesen wird, am 26.5.2020 zugegriffen).

2 Bundesministerium der Verteidigung (BMVg), *Konzeption der Bundeswehr*, Berlin: Bundesministerium der Verteidigung, Juli 2018, <https://bit.ly/2CTH2YV>.

3 David Sanger, *The Perfect Weapon. War, Sabotage, and Fear in the Cyber Age*, New York/Melbourne/London, 2018.

4 Joshua Rovner, »Cyber War as an Intelligence Contest«, *War on the Rocks*, 16.9.2019, <https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/>.

5 Bundesregierung, *Weißbuch* [wie Fn. 1], S. 36f.

6 Deutscher Bundestag, 19. Wahlperiode, *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Alexander Graf Lambsdorff, Grigorios Aggelidis, Renata Alt, weiterer Abgeordneter und der Fraktion der FDP*, 9.8.2019, Drucksache 19/11734, <http://dipbt.bundestag.de/dip21/btd/19/122/1912235.pdf>.

eher begrenzten Szenarien wie der Unterstützung von Truppen in Kampfsituationen. Aber nicht alles, was technisch möglich ist, ist für Deutschland geboten, operativ umsetzbar, rechtlich erlaubt oder sinnvoll, auch eingedenk des eher defensiven außenpolitischen Profils der Bundesrepublik, die ihren Fokus auf Krisenprävention und Konfliktmanagement richtet.

Diese Unklarheit ist aus mehrerlei Gründen problematisch: Erstens schadet die Ungewissheit, welchen Sinn und Zweck die militärischen Cyber-Operationen erfüllen sollen, der Legitimierung des geplanten Vorgehens vor der eigenen Bevölkerung. Unklarheit führt zu Fehlwahrnehmungen. In öffentlichen Diskursen wird teilweise sehr wild spekuliert, etwa dass Deutschland »offensive Cyberkriege« plane, obwohl sich das nicht mit der Realität deckt.

Zweitens wirkt sich die Unklarheit negativ auf die Effektivität der in Rede stehenden Einsätze im Cyber- und Informationsraum aus: Wenn wir nicht wissen, wofür die Bundeswehr Cyber-Operationen durchführen will, können wir auch nicht abschätzen, ob diese Einsatzzwecke überhaupt wirksam, risikoarm und sicherheitspolitisch sinnvoll sind. Wenn keine Erkenntnisse darüber vorliegen, unter welchen Voraussetzungen Cyber-Operationen militärisch funktional sind, versagt das Mittel im schlimmsten Fall in Konfliktsituationen, weil die Rahmenbedingungen falsch eingeschätzt wurden. Das Problem ist vergleichbar mit der Diskussion über das G36-Sturmgewehr, das für mitteleuropäische Temperaturen entwickelt, aber unter anderen klimatischen Rahmenbedingungen eingesetzt wurde und dort schnell überhitzte.[7] Andere Cyber-Akteure haben diese Erfahrungen bereits gemacht.

Wenn wir Einsatzbedingungen, operative Beschränkungen und etwaige Folgeeffekte eigener Cyber-Operationen falsch einschätzen, ergeben sich überdies enorme Risiken für Kollateralschäden, etwa in Form einer ungewollten Beeinträchtigung der zivilen kritischen Infrastruktur in Drittländern. Hieraus können sich ungünstige Eskalationsdynamiken ergeben.

Drittens haben die Folgen der Unklarheit auch eine rechtliche Dimension, denn nicht alle Arten von OMCO werden völkerrechtlich und grundrechtlich legitim sein. In einer Bundestagsanhörung zum Thema kritisierte der Völkerrechtler Michael Bothe, dass immer nur pauschal diskutiert werde, ob die Bundeswehr *generell* im Cyber-Raum aktiv sein darf oder nicht.[8] Diese Frage kann aber nicht pauschal beantwortet werden, da etwa das Erfordernis des Parlamentsvorbehalts von den *speziellen Charakteristika,* also der konkreten Ausgestaltung der geplanten Cyber-Operationen, abhängt. Nicht alle OMCO haben etwa die Eigenschaft einer »bewaffneten Unternehmung«, die ein Kernkriterium für eine parlamentarische Zustimmung ist.[9] Großflächige Sabotage-Angriffe auf kritische Infrastrukturen in Friedenszeiten haben zum Beispiel andere Wehr- und Völkerrechtsimplikationen als Spionageangriffe. Es ist daher sinnvoller zu fragen, *welche Arten* von OMCO legitim sind und welche nicht. Da aber das BMVg kaum öffentlich kommuniziert, welche OMCO-Varianten man selbst durchführen will, gibt es bisher keine Fälle, an denen man die grundrechtlichen und völkerrechtlichen Fragestellungen durchspielen könnte. Daher steckt die Debatte seit 2016 fest.

Am Anfang der vorliegenden Studie steht die Analyse einer Reihe von Fällen der militärischen Nutzung von Cyber-Operationen anderer Staaten. Daraus wird eine Typologie entwickelt. Diese Typologie soll klären, welche prototypischen OMCO es gibt und welche davon für Deutschland sicherheitspolitisch sinnvoll und vor allem grundrechtlich unproblematisch sind. Zwei Fragen stehen dabei im Vordergrund:

1 Was ist im Allgemeinen der Nutzen offensiver militärischer Cyber-Operationen und welchen operativen Begrenzungen unterliegen sie?
2 Inwiefern passen OMCO zum spezifischen Aufgabenprofil der Bundeswehr und welche Hindernisse gibt es?

Die Frage, welchen Sinn und Zweck *zivile* Cyber-Angriffe im Rahmen der aktiven Cyber-Abwehr haben können, wird daher bewusst außer Acht gelassen.[10]

7 Gabriel Borrud, »›An der G36 ist absolut nichts falsch!‹«, *Deutsche Welle* (online), 24.4.2015, <https://www.dw.com/de/an-der-g36-ist-absolut-nichts-falsch/a-18403289>.

8 Michael Bothe, *Stellungnahme zu Rechtsfragen des Cyberwar für den Verteidigungsausschuss des Deutschen Bundestages*, Deutscher Bundestag, 2016 (Nr. 18[12]633), 17.2.2016, <https://www.bundestag.de/resource/blob/408624/6b1ae626c3347d0ee38db6994aaf3941/stellungnahme-bothe-data.pdf>.

9 *Gesetz über die parlamentarische Beteiligung bei der Entscheidung über den Einsatz bewaffneter Streitkräfte im Ausland. Parlamentsbeteiligungsgesetz*, 2005, <https://bit.ly/2BXp0Va>.

10 Siehe etwa Thomas Reinhold / Matthias Schulze, *Digitale Gegenangriffe. Eine Analyse der technischen und politischen Implikationen von »hack backs«*, Berlin: Stiftung Wissenschaft und Politik, 2017 (Arbeitspapier FG03-AP Nr. 1), <https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/AP_Schulze_Hackback_08_2017.pdf>.

Militärische Cyber-Operationen

Als offensive militärische Cyber-Operationen (OMCO) bezeichnet man eine Sequenz koordinierter, mit digitalen Mitteln ausgeführter Cyber-Angriffe, um ein militärisches Ziel zu erreichen.[11] Als militärisch sind solche Operationen dann zu werten, wenn sie

a) von militärischen Akteuren wie Cyber-Kommandos ausgeführt werden;
b) eine militärische Funktion haben, zum Beispiel die Schädigung militärischer Infrastrukturen oder Waffensysteme, und
c) innerhalb eines bewaffneten Konflikts, etwa im Verbund mit konventionellen Einheiten, stattfinden.

Von den Millionen Cyber-Vorfällen, die jedes Jahr dokumentiert werden, sind nur eine Handvoll als militärische Operationen einzustufen.

Von den Millionen Cyber-Vorfällen, die jedes Jahr dokumentiert werden, sind nur eine Handvoll als militärische Operationen einzustufen.[12] OMCO lassen sich anhand ihrer Wirkung, das heißt anhand ihrer ausgelösten Effekte, typologisieren. Diese Einteilung leitet sich aus der völkerrechtlichen Literatur ab: Insbesondere westliche Völkerrechtler gehen davon aus, dass vor allem die Art und der Umfang der Effekte von Cyber-Angriffen darüber bestimmen, ob diese nach dem Völkerrecht als Gewalteinsatz oder gar als bewaffneter Angriff zu bewerten sind.[13] Bei einem Cyber-Angriff, der die Intensität und/oder den Umfang eines konventionellen bewaffneten Angriffs erreicht, kann zum Beispiel das Recht auf Selbstverteidigung greifen (UN-Charta Art. 51).[14] Das ist etwa dann der Fall, wenn der Angriff eine großflächige physische Zerstörung und den Verlust von Menschenleben nach sich zieht. Bisher gibt es nur sehr wenige Cyber-Vorfälle, bei denen jemals diese Schwelle erreicht wurde. Bei der Bestimmung dieser Schwelle gibt es im Übrigen erhebliche Interpretationsspielräume. Auch nicht-zerstörerische Cyber-Angriffe mit entsprechend großer Breitenwirkung, etwa eine zeitgleiche Störung europäischer Flugverkehrskontrollsysteme, können große Schäden anrichten. Zudem ist Cyber-Spionage nach dem Völkerrecht zwar nicht geächtet, kann aber der Vorbereitung zerstörerischer Effekte dienen. Um diese Grauzone auszuleuchten, bietet es sich an, Cyber-Operationen anhand ihrer Wirkung zu unterscheiden.

11 Jelle van Haaster, *On Cyber. The Utility of Military Cyber Operations During Armed Conflict*, Amsterdam: Amsterdam Center for International Law, 2019, S. 191.

12 Paolo Passeri, »December 2019 Cyber Attack Statistics«, *Hackmageddon* (online), 15.1.2020, <https://www. hackmageddon.com/2020/01/15/december-2019-cyber-attack-statistics/>.

13 Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*, Cambridge/New York: Cambridge University Press, 2013, S. 47ff. Allerdings teilen Staaten wie Russland und China diese Rechtsinterpretation nicht.

14 Ebd.

Infokasten
»Typologie militärischer Cyber-Operationen nach Nutzungszweck«

Die **Defensive Nutzung** militärischer Cyber-Operationen zielt darauf ab, digitale Fähigkeiten zu erhalten und eigene Daten, Netzwerke und Systeme zu schützen. Die Operationen können *passiv*-defensiv sein, sich also auf das eigene Netzwerk beschränken (passive Cyber-Abwehr bzw. Aufbau von IT-Sicherheit und Resilienz). Oder sie sind *aktiv* bzw. offensiv, das heißt, sie wirken in fremden Netzwerken, um Angriffe an der Quelle zu unterbinden (zivile aktive Cyber-Abwehr bzw. militärische Cyber-Verteidigung). Die Bundesregierung unterscheidet zwischen ziviler *Cyber-Abwehr,* die durch das Bundesministerium des Innern und nachgeordnete Behörden sichergestellt wird, und *militärischer Cyber-Verteidigung* innerhalb der rechtlichen Parameter des Streitkräfteeinsatzes. Unter technischen Gesichtspunkten sind damit aber sehr ähnliche Praktiken gemeint. Aktive Cyber-Abwehr und militärische Cyber-Verteidigung nutzen beide offensive Angriffspraktiken in fremden Systemen, allerdings mit defensiver Intention als Reaktion auf einen vorausgegangenen Cyber-Angriff. Allerdings ist die Intention bei Cyber-Angriffen nur selten eindeutig bestimmbar, so dass auch defensiv intendierte Reaktionen auf Cyber-Angriffe in der Regel als eigenständige, offensive und unfreundliche Handlungen wahrgenommen werden.[a]

Offensive Militärische Cyber-Operationen (OMCO) sind Maßnahmen jenseits der eigenen Verteidigung. Dabei handelt es sich um eine Form der Machtprojektion mit Hilfe digitaler Technologien, die in der Regel im Cyber-Raum erfolgt und überwiegend in fremden Netzwerken stattfindet. Es können die folgenden *Effekte* auftreten, die natürlich auch kombiniert werden können:

- **Denial & Disruption (Nichtverfügbarkeit):** Ein Gegner wird temporär an der Nutzung seiner Ressourcen gehindert. Das geschieht etwa, wenn Zugang zu einer Ressource gesperrt ist, der Strom ausfällt oder Server bis zur Abschaltung mit Anfragen geflutet werden (Denial of Service, DoS). Disruptionen verursachen nur geringe, reversible und meist temporäre Schäden.[b]
- **Zerstörung** ist die nicht-reversible Form der Nichtverfügbarkeit. Diese Effekte verursachen in der Regel beim Gegner die meisten Kosten.[c] Erstens können einzelne *Daten* gelöscht werden, was nur dann irreversibel ist, wenn keine Backups existieren. Zweitens können *Computer* in der Art »zerstört« werden, dass ihre Festplatten oder Startprozesse (»Master Boot Record«) gelöscht oder ihre Komponenten überhitzt werden.[d] Drittens kann damit ein *kinetischer Effekt* gemeint sein, der durch cyber-physische Systeme, wie industrielle Steuerungsanlagen, ausgelöst wird, die an den Zielcomputer angeschlossen sind. Die *Stuxnet*-Schadsoftware, die in iranische Atomzentrifugen eingeschleust wurde, ist hier das bisher eindrucksvollste Beispiel.
- **Manipulation** meint die Veränderung von Daten und Informationssystemen des Gegners (»Integritätsverlust« im IT-Jargon). Das kann in der Form des Einspeisens von falschen Zielkoordinaten in ein Raketensystem passieren oder auch durch die Veränderung elektronischer Wahlregister. Strenggenommen ist Manipulation eine Metakategorie, da auch bei Sabotage oder Informationsoperationen Daten manipuliert werden.
- **Intelligence, Surveillance, Reconnaissance (ISR):** Dieser Typus schließt Aktivitäten ein, die der Informationssammlung dienen mit dem Ziel, die militärische Planung zu unterstützen. ISR-Operationen können das Ausforschen von Informationen über Strategien, Ziele, Truppenallokation, Fähigkeiten und Intentionen eines Gegners und das Erstellen von Lagebildern (»situational awareness«) umfassen.[e] Im nichtmilitärischen Jargon wird dies Cyber-Spionage bzw. in der Nato »Computer Network Exploitation« (CNE) genannt, die auch von Nachrichtendiensten betrieben wird.[f] Technisch sind ISR und CNE nicht zu unterscheiden. Allerdings konzentriert sich militärische ISR in der Regel auf militärische Ziele, nachrichtendienstliche Spionage auf politische bzw. wirtschaftliche Ziele. ISR kann auch zur »preparation of the battlefield« verwendet werden, also dazu dienen, ein System präemptiv zu manipulieren mit dem Ziel, einen verdeckten Hintertürzugang zu platzieren, der im Fall einer späteren militärischen Eskalation ausgenutzt werden kann.[g] Die aktuelle US-Cyber-Strategie spricht in diesem Kontext von Vorwärtsverteidigung im gegnerischen Netzwerk.
- **Informations-Operationen (InfoOps):** Im Nato-Jargon sind InfoOps »eine militärische Funktion, die der Koordination militärischer Informationsaktivitäten dient, um zur Unterstützung der Ziele der Bündnismission gewünschte Auswirkungen auf den Willen, das Verständnis und die Fähigkeiten von Gegnern, potentiellen Gegnern und anderen Parteien herbeizuführen«.[h] Bei InfoOps geht es also darum, den politischen Willen eines Zielpublikums zum eigenen Vorteil zu beeinflussen. Digitale InfoOps können auf wahren Informationen beruhen, das heißt nicht-irreführend sein und sich auf die Verbesserung des eigenen Images beziehen (weiße Propaganda / Public Relations bzw. strategische Kommunikation), oder bewusst irreführend und den Urheber verschleiernd sein und auf negative, destabilisierende Effekte abzielen (Desinformation bzw. aktive Maßnahmen). Russland setzt Informationsoperationen strategisch gegen ganze Bevölkerungen ein, während westliche Staaten diese eher taktisch einsetzen.[i] Eine Unterform von InfoOps sind psychologische Operationen (PsyOps), die Angst, Unsicherheit und Zweifel über die Integrität der eigenen Systeme schüren sollen.[j] Cyber- und Informationsoperationen wird in vielen Ländern gleich viel Bedeutung zugemessen.

Infokasten
»Typologie militärischer Cyber-Operationen nach Nutzungszweck« (Fußnoten)

a Ben Buchanan, *The Cybersecurity Dilemma. Hacking, Trust and Feat between Nations*, Bd. 1, Oxford: Oxford University Press, 2017, S. 20.

b Brandon Valeriano / Benjamin Jensen / Ryan C. Maness, *Cyber Strategy. The Evolving Character of Power and Coercion*, New York: Oxford University Press, 2018.

c Die Bundesregierung verwendet in einer Antwort auf eine Kleine Anfrage eine ähnliche Unterteilung, siehe Deutscher Bundestag, 18. Wahlperiode, *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Wolfgang Gehrcke, Christine Buchholz, weiterer Abgeordneter und der Fraktion DIE LINKE,* 11.3.2015, Drucksache 18/4286, <https://dip21.bundestag.de/dip21/btd/18/042/1804286.pdf>.

d Andy Greenberg, »The Untold Story of NotPetya, the Most Devastating Cyberattack in History«, *Wired* (online), 22.8.2018, <www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.

e Van Haaster, *On Cyber* [wie Fn. 11].

f NATO, *AAP-06. Edition 2018*, Brüssel 2018, <https://standards.globalspec.com/std/10275442/AAP-06>.

g Antoine Lemay / Scott Knight / Jose Fernandez, »Intelligence Preparation of the Cyber Environment (IPCE). Finding the High Ground in Cyberspace«, in: *Journal of Information Warfare*, 13 (2014) 3, S. 46–56.

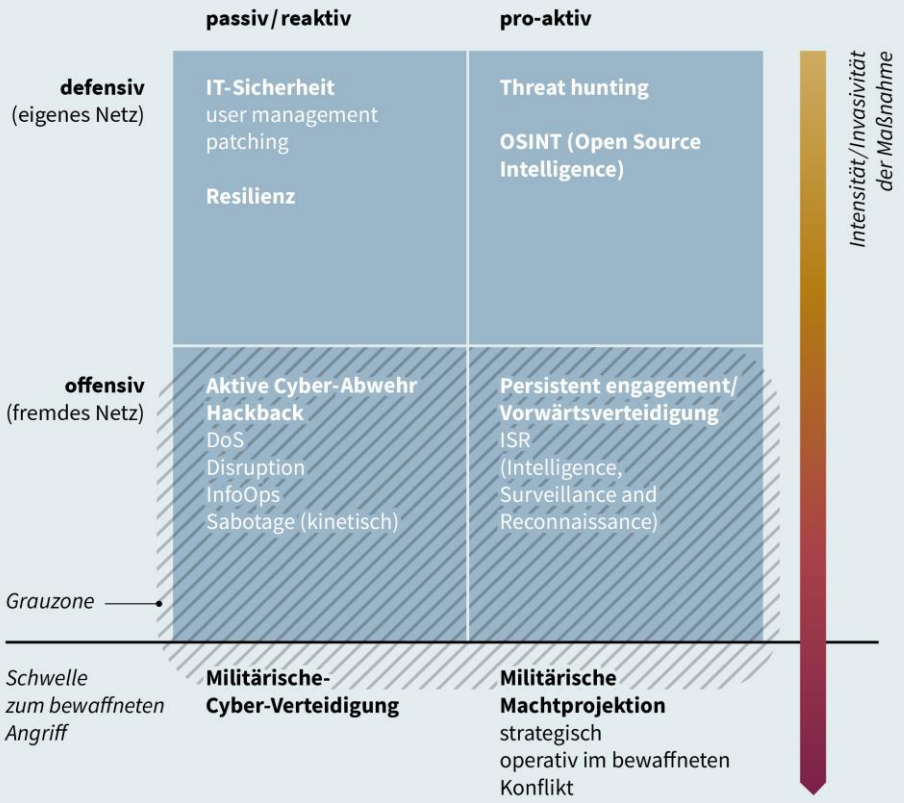
h NATO, *AAP-06* [wie Fn. f].

i Alexander Klimburg, *The Darkening Web. The War for Cyberspace*, New York: Penguin Press, 2017, S. 211.

j James A. Lewis, »›Compelling Opponents to Our Will‹: The Role of Cyber Warfare in Ukraine«, in: Kenneth Geers (Hg.), *Cyber War in Perspective: Russian Aggression against Ukraine*, Tallinn 2015, S. 39–48.

Grafik 1

Cyber-Operationen: Übersicht über die wichtigsten Begriffe



Die Bundeswehr im Cyber- und Informationsraum

Am 17. September 2015 erließ die damalige Verteidigungsministerin Ursula von der Leyen den Tagesbefehl zur Errichtung »des neuen militärischen Organisationsbereichs Cyber- und Informationsraum«.[15] Der dazu berufene Aufbaustab sollte einerseits ein neues Organisationselement Cyber/IT im Bundesverteidigungsministerium und andererseits den Organisationsbereich »Cyber- und Informationsraum« in der Bundeswehr konzipieren. Begründet wurde die Entscheidung für diese Maßnahme mit dem strategischen Kontext, konkret mit der Existenz neuartiger (hybrider) Gefahren aus dem Cyber- und Informationsraum, insbesondere in Gestalt von »Advanced Persistent Threats« (APT, dt. Hochentwickelte, anhaltende Bedrohungen). Für die Bundeswehr als Betreiber zahlreicher IT-Systeme, von Kommunikationsnetzen bis Waffensystemen, ergab sich daraus die Notwendigkeit, ihre eigene Informationstechnik und ihre digitale Handlungsfähigkeit als Hochwertziel zu schützen. Damit ging neben einer stärkeren Beschäftigung mit IT-Sicherheit auch ein Modernisierungsanspruch einher: Zahlreiche verstreute IT-Komponenten der Bundeswehr sollten konsolidiert werden. 13 500 Dienstposten, die sich über verschiedene Bundeswehreinheiten verteilten, wurden in dem neuen Organisationsbereich gebündelt, der seither von dem Kommando Cyber- und Informationsraum (KdoCIR) geleitet wird. Zum KdoCIR gehören rund 260 zivile und militärische Dienstposten.[16] Die Entwicklung des gesamten Organisationsbereichs soll in einem mehrstufigen Prozess stattfinden, der den Planungen zufolge 2021 mit einer Personalstärke von 14 000 abgeschlossen ist.

Die Aufstellung von Cyber-Fähigkeiten wurde auch mit dem Verweis auf die Entwicklungen bei den Bündnispartnern in der Nato begründet. Aus den Cyberschutzaktivitäten der Alliierten ergeben sich für die Bundeswehr Anforderungen an die Gewährleistung der gemeinsamen Abschreckung, der Streitkräfteintegration in multinationalen Verbänden und allgemein an die Interoperabilität.[17] Die Nato betrachtet den »Cyberspace« seit 2016 als eine eigene Domäne des Krieges, neben Luft, Wasser und Land. Damit verbunden sind bestimmte Anforderungen an das Fähigkeitsprofil der Bundeswehr. Grob zusammengefasst wurden die folgenden Handlungsfelder identifiziert:[18]

1. Schutz der IT-Systeme der Bundeswehr. Dazu gehören das Sichern der Versorgungsketten, eigenständiges Erforschen und Entwickeln von Schlüsseltechnologien, das Rekrutieren und Ausbilden von IT-Fachpersonal in Studiengängen und das Weiterbilden des bestehenden Personals.
2. Mitwirkung beim Schutz kritischer Infrastrukturen im Rahmen der gesamtstaatlichen Sicherheitsvorsorge und Erstellung einer militärischen Nachrichtenlage als Beitrag zum gesamtstaatlichen Lagebild.
3. Durchführung von Computer-Netzwerk-Operationen, elektronische Kampfführung und Identifizierung von Desinformationskampagnen in Krisengebieten und im Rahmen mandatierter Einsätze.

15 BMVg, *Tagesbefehl zur Aufstellung des neuen militärischen Organisationsbereichs Cyber- und Informationsraum der Bundeswehr*, 17.9.2015.

16 BMVg, *Aufstellung Kommando CIR: Ein Meilenstein deutscher Sicherheits- und Verteidigungspolitik*, 5.4.2017, <https://www.bmvg.de/de/aktuelles/aufstellung-kommando-cir-11120>.

17 BMVg, *Abschlussbericht Aufbaustab Cyber- und Informationsraum. Empfehlungen zur Neuorganisation von Verantwortlichkeiten, Kompetenzen und Aufgaben im Cyber- und Informationsraum sowie ergänzende Maßnahmen zur Umsetzung der Strategischen Leitlinie Cyber-Verteidigung*, Berlin, April 2016, <http://docs.dpaq.de/11361-abschlussbericht_aufbaustab_cir.pdf>.

18 Manuel Ladiges, »Der Cyberraum — ein (wehr)verfassungsrechtliches Niemandsland?«, in: *Neue Zeitschrift für Wehrrecht*, 59 (2017) 6, S. 221—245.

Grafik 2

Cyber-Entwicklungen bei der Bundeswehr

Insbesondere auf den dritten Punkt richtet sich das Interesse dieser Studie. Das Zentrum Cyber-Operationen (ZCO) in Rheinbach, das für OMCO zuständig ist, umfasst rund 100 zivile und militärische Dienstposten.[19]

Genese und Funktion offensiver Cyber-Fähigkeiten in den strategischen Dokumenten der Bundeswehr

Deutschland hat keine Cyber-Doktrin, also kein Dokument, das die Grundprinzipien für das Handeln von Streitkräften im Cyberraum fixieren würde. Die strategischen Überlegungen zur Nutzung von OMCO sind, anders als etwa bei der US-Behörde CYBERCOM, nicht an einer Stelle gebündelt, sondern über verschiedene Schriftstücke verteilt.[20] Diese Dokumente werden im Folgenden untersucht. Dabei wird analysiert, für welche Zwecke die Bundeswehr OMCO vorsieht bzw. welche militärischen Ziele damit erreicht werden sollen, welche Arten von OMCO durchgeführt werden sollen und wie sich dieses Instrument in die deutsche Sicherheitspolitik einfügt.

Die ersten Erwägungen, dass die Bundeswehr OMCO einsetzen könnte, gehen auf das Jahr 2011 zurück, in dem unter Federführung des Innenministeriums auch die erste deutsche Cyber-Sicherheitsstrategie veröffentlicht wurde. In den *Verteidigungspolitischen Richtlinien* des Bundesverteidigungsministeriums von 2011 wird erstmals die strategische Bedrohung erwähnt, die von Informationstechnologien ausgehen kann, insbesondere wegen der dadurch eröffneten Chancen für Cyber-Kriminalität, Desinformation oder Cyber-Angriffe auf kritische Infrastrukturen. Die *Richtlinien* enthalten aber keine konkreten Ausführungen dazu, wie diesen Bedrohungen begegnet werden könnte.[21]

Konkreter wird indes ein von WikiLeaks veröffentlichter, nur für den Dienstgebrauch bestimmter *Bericht des BMVg an den Verteidigungsausschuss 2013*, in dem schon ausführlichere Überlegungen zur Funktion und zu den rechtlichen Rahmenbedingungen von Bundeswehr-OMCO angestellt werden. Dem *Bericht* zufolge geht das BMVg davon aus, dass ein strategischer Cyber-Krieg, im Sinne eines digitalen Überraschungsangriffs auf zivile Infrastrukturen, der eine gesamte Gesellschaft für einen längeren Zeitraum lahmlegt, ein unrealistisches Szenario ist. Vielmehr bereite sich die Bundeswehr auf Szenarien vor, in denen Cyber-Attacken im Kontext eines konventionellen Angriffs begleitend eingesetzt werden.[22] Eigene OMCO der Bundeswehr sollen vornehmlich zur Verteidigung im Falle eines bewaffneten Angriffs auf die Bundesrepublik (Grundgesetz [GG] Artikel 87a bzw. UN-Charta Art. 51), zur Unterstützung laufender militärischer Auslandseinsätze (GG Art. 24) und zur Abwehr von menschengemachten Unglücksfällen im Innern (GG Art. 35) in Betracht kommen. Der Verweis auf diese grundgesetzlichen Rahmenbedingungen ist seither in allen Dokumenten zu finden, in denen Offensive militärische Cyber-Operationen thematisiert werden. OMCO im Rahmen von Auslandseinsätzen erfordern einen Parlamentsbeschluss und müssen sich an den Prinzipien des Völkerrechts orientieren.[23] Konkrete Einsatzzwecke werden in dem *Bericht* nicht diskutiert, allerdings wird darauf hingewiesen, dass mit OMCO im Falle eines militärischen Einsatzes vornehmlich passive Aufklärungszwecke verfolgt werden sollen.[24] Explizit wird hier betont, dass dies auch schädigende, das heißt disruptive oder destruktive Effekte für IT-Systeme oder Daten eines Gegners einschließen kann.[25]

In der geheimen *Strategischen Leitlinie Cyber-Verteidigung* von 2015, die Netzpolitik.org veröffentlicht hat, werden die OMCO-Einsatzzwecke konkretisiert und erweitert.[26] Eine strategische Verwendung von OMCO

19 BMVg, *Abschlussbericht Aufbaustab Cyber- und Informationsraum* [wie Fn. 17].

20 US Department of Defense, *Department of Defense Cyber Strategy. Summary*, Washington, D.C., 2018, <https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF>.

21 BMVg, *Verteidigungspolitische Richtlinien. Nationale Interessen wahren – Internationale Verantwortung übernehmen – Sicherheit gemeinsam gestalten*, 27.5.2011, <www.bmvg.de/resource/blob/13568/28163bcaed9f30b27f7e3756d812c280/g-03-download-die-verteidigungspolitische-richtlinien-2011-data.pdf>.

22 BMVg, *Bericht zum Themenkomplex Cyber-Verteidigung*, Berlin 2013, S. 4ff, via WikiLeaks <https://bit.ly/3eSYbjy>. Da die Bundesregierung im Cyber-Bereich auf Geheimhaltung setzt und entsprechende Analysen nicht selbst veröffentlicht, muss auf solche kritisch zu betrachtenden Sekundärquellen zurückgegriffen werden.

23 Ebd., S. 15ff.

24 Ebd., S. 19ff.

25 Ebd., S. 16.

26 BMVg, *Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg*, Berlin, 16.4.2015, via Netzpolitik.org <https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-

in Friedenszeiten ist nicht geplant. Die verfassungsrechtlichen Grundlagen dafür sollen nun aber immerhin geprüft werden. Das Ziel des Einsatzes von OMCO, so heißt es in dem Dokument, bestehe in der Erstellung von Lagebildern zu den eigenen Fähigkeiten und Systemen zur Einsatzunterstützung. Allerdings soll mit Hilfe von OMCO auch ein Lagebild zu den gegnerischen Systemen beschafft werden, das Informationen über gegnerische Fähigkeiten, Verwundbarkeiten und Angriffsvektoren aufzeigt. Das legt den Schluss nahe, dass OMCO für die Bundeswehr nicht nur dazu dienen sollen, Informationen für passiv-defensive Zwecke zu sammeln, sondern auch dazu, aktiv durch eigene Cyber-Spionage erhobene Schwachstellen gegnerischer Systeme ausfindig zu machen. Damit würde die Bundeswehr OMCO im Sinne einer ISR-Funktion (Intelligence, Surveillance and Reconnaissance) einsetzen, was auch vorbereitende Aktionen in fremden Netzen einschließen könnte. In dem Dokument wird explizit erwähnt, dass auch der BND Informationen beschaffen kann, etwa über unbekannte 0-Day-Schwachstellen in gegnerischer Software. Diese Erkenntnisse könnten auch der Bundeswehr bei der Vorbereitung ihrer Aufgaben helfen. Ob und wie dieser Austausch operativ abläuft und rechtlich ausgestaltet ist, bleibt unerwähnt. Neben ISR sollen OMCO auch dazu eingesetzt werden, den Gegner bei der Nutzung des Cyber- und Informationsraums zu behindern, ihm dessen Nutzung ganz zu verwehren oder die Nichtverfügbarkeit von Systemen herbeizuführen. So sollen zum Beispiel gegnerische Kommunikationssysteme gestört werden.

In den *Strategischen Leitlinien* werden OMCO als »unterstützendes, komplementäres und substituierendes Wirkmittel« bezeichnet. Allerdings bleibt unklar, welche militärischen Funktionen Cyber-Angriffe ersetzen sollen. Denkbar wären vor allem Tools, die störende elektromagnetische Effekte auslösen. OMCO sollen den Handlungsspielraum der Bundeswehr erweitern und als »force multiplier« dienen. Weiter ausgeführt wird dies nicht. OMCO sollen im Inland vorbereitet und entwickelt werden, »spätestens« dann, wenn das Einsatzmandat erteilt wird, was aber impliziert, dass eine technische Vorausentwicklung von Angriffsfähigkeiten gewünscht wird, schon bevor ein Parlamentsmandat existiert.[27]

In einer Antwort auf eine Kleine Anfrage aus demselben Jahr hat die Bundesregierung diese Punkte ergänzt: Strategischer »›Cyberwar‹ ist kein Konzept für die Bundeswehr«, heißt es dort. Cyber-Mittel sollen stattdessen im Verbund eingesetzt werden. Die damit verknüpften Ziele seien der Schutz der eigenen Kräfte und die Erhöhung der Wirkung anderer Waffensysteme. Wie genau diese Absichten taktisch umgesetzt werden sollen, kann aber erst bestimmt werden, wenn ein Einsatzmandat vorliegt, welches Ziele, Möglichkeiten und Grenzen des Handelns definiert.[28]

Eine Erweiterung des Einsatzspektrums für OMCO findet sich schließlich in dem 2016 fertiggestellten *Abschlussbericht* des Stabes, der mit dem Aufbau des Cyber- und Informationsraums (CIR) betraut war. Die Verfasser erweitern die Palette der potentiellen OMCO-Einsätze um das Einwirken auf gegnerische Informationen und auf die Beeinflussung des Informationsumfelds. Bei solchen Operationen geht es darum, Propaganda und Desinformationsaktivitäten in Krisengebieten zu identifizieren und eine »Teilhabe an der Meinungsbildung im Informationsumfeld der Interessengebiete der Bundeswehr und in mandatieren Einsätzen« sicherzustellen[29] Diese Ausführungen müssen vor dem Hintergrund der Beeinflussungsversuche russischer Hacker im US-Wahlkampf 2016 gesehen werden. Geht es nach dem *Abschlussbericht*, dann ist es das Ziel von Bundeswehr-OMCO, eine »Informationsdominanz« im Cyber- und Informationsraum zu erlangen, um militärische Entscheidungsprozesse und auch die Einsatzwirkung zu verbessern. Das Augenmerk richtet sich also viel stärker auf Informationsoperationen und weniger, wie zuvor, auf die Unterbindung bzw. die Behinderung gegnerischer Kommunikation. Eigenständige strategische OMCO (ohne einen begleitenden konventionellen Streitkräfteeinsatz) mit disruptiven Effekten seien zwar denkbar, allerdings »sind die über den CIR erzielbaren Effekte grundsätzlich Teil einer streitkräftegemeinsamen Operation«.[30] Der Fokus liegt somit weiterhin auf OMCO in konventionellen Einsätzen und nicht auf der strategischen Beeinflussung von Gegnern in Friedenszeiten.

digitale-angriffe/>. Das Dokument wurde nur digital veröffentlicht und besitzt keine zitierbaren Seitenzahlen.

27 Ebd.

28 Deutscher Bundestag, 18. Wahlperiode, *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Alexander S. Neu, Andrej Hunko, Wolfgang Gehrcke, weiterer Abgeordneter und der Fraktion DIE LINKE*, 10.12.2015, Drucksache18/6989, <https://dipbt.bundestag.de/dip21/btd/18/069/1806989.pdf>.

29 BMVg, *Abschlussbericht Aufbaustab Cyber- und Informationsraum* [wie Fn. 17], S. 13.

30 Ebd.

Am konkretesten wird die *Konzeption der Bundeswehr* aus dem Jahr 2018. Das »Dachdokument für die Gesamtkonzeption der militärischen Verteidigung Deutschlands« legt den Auftrag, die Aufgaben und die Fähigkeiten der Streitkräfte fest.[31] Deutschland müsse, so ist in dem Leitfaden zu lesen, aufgrund der Einbettung in das Rahmennationkonzept der Nato[32] »über das gesamte Fähigkeitsspektrum im Verbund von Führung, Aufklärung, Wirkung und Unterstützung verfügen«.[33] Was sie damit meint, hat die Bundesregierung in einer Antwort auf eine Kleine Anfrage erläutert: »Unter einem vollen Fähigkeitenspektrum im Bereich Cyber-Sicherheit werden die Fähigkeiten verstanden, die zum Schutz eigener Informationen, IT sowie Waffen- und Wirksysteme dienen oder mit denen im Rahmen der Einsatz- und Operationsführung im und durch den Cyber- und Informationsraum gewirkt wird.«[34] Damit sind alle Typen von OMCO abgedeckt, die oben beschrieben wurden (siehe Kapitel »Militärische Cyber-Operationen«). Handlungsleitend für die Bundeswehr ist demnach ein vernetzter Ansatz, bei denen OMCO im Verbund mit Instrumenten der staatlichen Sicherheitsvorsorge im Krisenmanagement eingesetzt werden.

Die Bundeswehr darf erst aktiv werden, wenn hybride Aktivitäten eine bestimmte Schwelle erreichen, was sie erfahrungsgemäß nicht tun.

Im Hinblick auf die im Dienste der Landesverteidigung abzuwehrenden Bedrohungen wird davon ausgegangen, dass Angreifer, ähnlich wie in Georgien 2008, hybride Methoden wie Subversion, Desinformation und Cyber-Fähigkeiten unterhalb der Schwelle eines bewaffneten Angriffs — und somit außerhalb des rechtlichen Aufgabenbereichs der Bundeswehr — einsetzen könnten. Aus diesem Umstand ergibt sich ein Spannungsfeld, denn die Bundeswehr darf erst aktiv werden, wenn ein bewaffneter Angriff vorliegt, sprich, wenn hybride Aktivitäten eine bestimmte Schwelle erreichen, was sie in der Empirie aber in der Regel nicht tun.[35] Klarer indes ist das Szenario einer großangelegten Cyber-Attacke, egal ob strategisch oder im Verbund mit konventionellen Streitkräften: Ein solcher Angriff kann einen Spannungs- oder Verteidigungsfall auslösen. Für die Bewältigung einer derartigen Krise benötige die Bundeswehr eine sofortige Reaktionsfähigkeit im gesamten Eskalations- und Wirkungsspektrum. Cyber-Fähigkeiten können eine Rolle bei der Erstellung eines Lagebilds spielen, auf dem wiederum die Einsatzplanung basiert. Konkret wird aber auch über Operationen nachgedacht, die den Gegner am Zugang zu bestimmten Ressourcen hindern. Eine Verwundbarkeit wird speziell bei führungsrelevanten Informationssystemen gesehen, die gestört oder gar physisch zerstört werden können.[36]

Cyber-Fähigkeiten sind aber auch eine Ergänzung zu militärischer Stärke im Krisenmanagement bei Out-of-area-Einsätzen. Die Erhebung krisenrelevanter Daten wird als Dauereinsatzaufgabe begriffen. Beim Heimatschutz fallen »Verteidigungsaspekte der gesamtstaatlichen Cyber-Sicherheit« in den Aufgabenbereich der Bundeswehr, zum Beispiel in Form subsidiärer Unterstützungsleistungen, wenn Behörden im Inland Amtshilfe anfragen. Dies geschieht aber nur auf Bedarfsbasis beim Schutz kritischer Infrastrukturen.

31 BMVg, *Konzeption der Bundeswehr* [wie Fn. 2], S. 4.

32 »Die Kernidee des Konzepts: Die Bundeswehr bietet vor allem kleineren europäischen Streitkräften einen Rahmen, in dem militärische Ressourcen zusammengeführt, gemeinsam geplant und beschafft werden. Zudem sollen die Partner mit Einheiten ihrer Streitkräfte in die Bundeswehr eingebunden werden können, um gemeinsame Großverbände zu bilden. So soll langfristig ein schlagkräftiger Verbund europäischer Armeen entstehen«; Björn Müller, *Das Rahmennationenkonzept*, Bonn: Bundeszentrale für politische Bildung, 2.5.2019 (Dossier Deutsche Verteidigungspolitik), <https://www.bpb.de/politik/grundfragen/deutsche-verteidigungspolitik/290423/rahmennationenkonzept>.

33 BMVg, *Konzeption der Bundeswehr* [wie Fn. 2], S. 7.

34 Deutscher Bundestag, 19. Wahlperiode, *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Agnieszka Brugger, Dr. Konstantin von Notz, Dr. Tobias Lindner, weiterer Abgeordneter und der Fraktion Bündnis 90/Die Grünen*, 17.7.2018, Drucksache 19/3420, <http://dip21.bundestag.de/dip21/btd/19/034/1903420.pdf>.

35 Genau diese rechtliche Grauzone sollte im Sommer 2019 mit der Diskussion über einen »digitalen Verteidigungsfall« ausgeleuchtet werden. Allerdings führte die Initiative des Inspekteurs Cyber- und Informationsraum (InspCIR) zu keiner Rechtsänderung, siehe Deutscher Bundestag, *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Alexander Graf Lambsdorff, Grigorios Aggelidis, Renata Alt* [wie Fn. 6].

36 BMVg, *Konzeption der Bundeswehr* [wie Fn. 2], S. 40.

Um diese Aufgaben erfüllen zu können, müssen laut *Konzeption der Bundeswehr* defensive und offensive Cyber-Fähigkeiten aufgestellt und kontinuierlich geübt und weiterentwickelt werden. Cyber-Fähigkeiten sollen im Verbund mit konventionellen Fähigkeiten, also Streitkräften, eingesetzt werden, »etwa durch die zeitlich koordinierte Beeinflussung gegnerischer Systeme und kritischer Infrastrukturen«.[37] OMCO gegen kritische Infrastrukturen anderer Länder, zum Beispiel gegen Energieversorger, gelten als besonders risikobehaftet, da hierbei physische Schäden entstehen und Menschenleben verlorengehen können.

Das »Spektrum an Wirkmitteln« reicht nach Auskunft der *Konzeption der Bundeswehr* »von einfachsten Ansätzen wie Sperren und Verminen über weitreichende Präzisionswaffen oder Maßnahmen des elektronischen Kampfes bis zu koordinierten Cyber-Aktivitäten«.[38] Im Vordergrund sollen für die Bundeswehr Aufklärungsfähigkeiten stehen, aber auch Anti-Access- und Area-Denial-Fähigkeiten, also Fähigkeiten zu Operationen, die den Zugang zu einem bestimmten Raum (Land, Luft, Wasser und Cyber) verhindern. Zudem werden in dem Dokument zwei neue Einsatzmodalitäten genannt: Cyber-Fähigkeiten zur elektronischen Kriegsführung und zur Austragung eines »Informationskampfs« im Kontext von Desinformationsbekämpfung: »Das Informationsumfeld als Bestandteil des Cyber- und Informationsraums ist derjenige Raum, in dem kognitive, sensorische, deutende, gedankliche und kommunikative Vorgänge stattfinden und aufgrund dessen Menschen Einstellung, Willen und Verhalten anpassen.«[39] Dieses Informationsumfeld soll analysiert werden, um im Rahmen des nationalen und internationalen Krisenmanagements Desinformation abwehren zu können.

Zusammengefasst zeigt sich, dass die strategischen Dokumente des BMVg zu OMCO sehr vage sind. Es bleibt im Dunkeln, welche Arten von OMCO man durchführen will und welche sicherheitspolitischen Ziele damit erreicht werden sollen. Das ist natürlich nachvollziehbar, wenn etwaigen Gegnern kein Informationsvorteil verschafft werden soll; für eine akademische und gesellschaftliche Diskussion ist es aber unbefriedigend, zumal andere Staaten hier transparenter agieren. In den Konzeptpapieren des BMVg finden sich nur diffuse Andeutungen dazu, für welche Ziele eigene OMCO eingesetzt werden sollen, etwa die Störung gegnerischer Kommunikationsinfrastrukturen. Was genau aber zum Beispiel »die Behinderung bzw. Verwehrung der gegnerischen Nutzung des Cyber- und Informationsraums« konkret bedeutet, ist unklar. Es gibt sehr unterschiedlich invasive, unterschiedlich kostspielige und völkerrechtlich bedenkliche Wege, dieses abstrakte Ziel zu erreichen. Der Umfang solcher Operationen kann gering sein und sich auf die gezielte Manipulation einzelner Server beschränken. Er kann aber auch gewaltig sein, wenn es sich um großflächige Angriffe gegen Internet-Infrastrukturen anderer Länder mit dem Effekt eines »Internet-Shutdown« handelt.

37 Ebd., S. 47.
38 Ebd.
39 Ebd., S. 51.

Strategisch, operativ, taktisch: Typen von OMCO am Beispiel anderer Länder

OMCO haben sehr verschiedene Charakteristika, die über Erfolgschancen und Risiken der Cyber-Operation bestimmen, aber auch Einfluss auf deren Rechtmäßigkeit haben. Das Ziel der folgenden Ausführungen ist, die Bandbreite unterschiedlicher OMCO aufzuzeigen, die von anderen Ländern bereits durchgeführt werden. Diese Analyse soll dabei helfen zu bestimmen, welche Zwecke Staaten mit welchen OMCO verfolgen und welche Hindernisse, seien sie operativer oder rechtlicher Art, es bei der Durchführung gibt. Damit sollen Beispiele für OMCO identifiziert werden, die sich Deutschland zum Vorbild nehmen könnte, da sie zu seinen außen- und sicherheitspolitischen Prioritäten passen. Zudem werden wichtige »lessons learned« extrahiert. Da OMCO für verschiedene strategische, operative oder taktische Ziele eingesetzt werden, erfolgt die Analyse anhand der Theorie von den drei Ebenen des Krieges. Dies ermöglicht es, die unterschiedlichen militärischen Aktivitäten besser zu ordnen.

Strategische OMCO

Unter strategischen Cyber-Angriffen versteht man solche, die darauf abzielen, das Verhalten bzw. das Kosten-Nutzen-Kalkül anderer Staaten als Ganzes zu beeinflussen. John Arquilla definiert strategischen Cyber-Krieg als ein »Mittel, um auf sehr kostspielige und störende Weise einen Gegner anzugreifen, ohne vorher gegnerische Streitkräfte im Feld, auf See oder in der Luft besiegen zu müssen«.[40] Das Ziel strategischer OMCO ist demnach, den Willen des Gegners und dessen Möglichkeiten zum Widerstand zu brechen oder dessen etwaige Angriffsabsichten zu beeinflussen, *ohne* konventionelle Streitkräfte verwenden zu müssen.[41] Beispiele dafür sind Angriffe auf kritische Infrastrukturen, vor allem auf vitale Funktionen eines Staates wie die Energieversorgung. Allerdings sind die meisten strategischen Cyber-Attacken bisher so konzipiert, dass sie unterhalb der völkerrechtlichen Schwelle eines bewaffneten Angriffs bleiben, um eine Eskalation zu einem konventionellen Konflikt zu vermeiden. Ein Großteil aller strategischen Cyber-Angriffe dient nicht genuin militärischen Zielen, sondern dem sogenannten »tacit bargaining«, also dem Kommunizieren politischer Botschaften durch Droh- oder Einschüchterungshandlungen.[42]

Ein Großteil aller strategischen Cyber-Angriffe dient nicht genuin militärischen Zielen, sondern dem sogenannten »tacit bargaining«.

Da Cyber-Fähigkeiten relativ neu sind, gibt es bis dato nur wenige Fälle, in denen OMCO strategisch und vor allem militärisch genutzt wurden, um einen Gegner zu besiegen.[43]

40 John Arquilla, »The Rise of Strategic Cyberwar?«, *Communications of the ACM* (online), 25.9.2017, <https://cacm.acm.org/blogs/blog-cacm/221308-the-rise-of-strategic-cyberwar/fulltext>.

41 James A. Lewis, »›Compelling Opponents to Our Will‹: The Role of Cyber Warfare in Ukraine«, in: Kenneth Geers (Hg.), *Cyber War in Perspective: Russian Aggression against Ukraine*, Tallinn 2015, S. 39–48.

42 Brandon Valeriano / Benjamin Jensen / Ryan C. Maness, *Cyber Strategy. The Evolving Character of Power and Coercion*, New York: Oxford University Press, 2018.

43 Erik Gartzke, »The Myth of Cyberwar. Bringing War in Cyberspace Back Down to Earth«, in: *International Security*, 38 (2013) 2, S. 41–73 (62).

Fallstudie *Nitro Zeus* 2016

Interessant ist die Operation *Nitro Zeus*, die US-CYBERCOM gegen den Iran plante und die 2016 vom *New-York-Times*-Journalisten David Sanger aufgedeckt wurde. Es handelte sich um einen Notfallplan für den Fall, dass die Vorgängeroperation *Olympic Games*, besser bekannt als *Stuxnet*, und die diplomatischen Bemühungen um eine Begrenzung des iranischen Atomprogramms gescheitert wären. Laut Sanger beinhaltete der Plan einen orchestrierten Cyber-Angriff auf Irans Luftverteidigungs-, Transport- und Kommunikationssysteme sowie auf wichtige Teile des Stromnetzes.[a] Der Präventivschlag sollte wohl auch zivile kritische Infrastruktur in Friedenszeiten lahmlegen. Sanger schreibt, dass *Nitro Zeus* eine großangelegte Aktion war, an der Tausende von Nachrichtendienstmitarbeitern beteiligt waren, die iranische Computernetzwerke infiltrierten, um das »Schlachtfeld vorzubereiten«. US-CYBERCOM verfügt über 6 000 Hacker in 133 »Mission Teams«. Insider bezeichnen die Operation als »ein riesiges, teures Unterfangen, das nur von wenigen Nationalstaaten umgesetzt werden kann«.[b] Zum Vergleich: Die Kosten des weitaus begrenzteren *Stuxnet*-Angriffs beliefen sich auf schätzungsweise 300 Millionen US-Dollar, bei einer circa fünfjährigen Entwicklungszeit.[c] Wie *Stuxnet* erforderte *Nitro Zeus* wahrscheinlich Jahre der Vorbereitung, Aufklärung, Simulation und Schadsoftware-Testung. Der Plan wurde nie ausgeführt.

a David Sanger / Mark Mazzetti, »U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict«, *New York Times* (online), 16.2.2016, <www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html>.
b David Sanger, *The Perfect Weapon. War, Sabotage, and Fear in the Cyber Age*, New York / Melbourne / London, 2018, S. 45.
c Brandon Valeriano / Ryan C. Maness, *Cyber War versus Cyber Realities. Cyber Conflict in the International System*, Oxford: Oxford University Press, 2015, S. 151.

Die Operation *Nitro Zeus*, die die US-Militärbehörde CYBERCOM gegen den Iran vorbereitete, liefert einige interessante »lessons learned« über Begrenzungen und Nutzen von strategischen OMCO: Erstens, so argumentiert Martin Libicki, sind strategische OMCO ungeeignet für zwei zentrale militärische Ziele, nämlich für die permanente Entwaffnung oder Zermürbung gegnerischer konventioneller Streitkräfte und die physische Besetzung eines Territoriums.[44] Gegnerische Guerilla-Kämpfer mit AK-74-Sturmgewehren und ohne eigene IT-Infrastruktur, ein Kombattanten-Typus, der in zahlreichen bewaffneten Konflikten auftritt, können mit Cyber-Attacken nicht besiegt werden. Da der Schaden, den diese verursachen, oft nur vorübergehend und reversibel ist, müssen meist dennoch konventionelle Streitkräfte eingesetzt werden, um einen Effekt zu verstetigen. Der militärische Nutzen von Cyber-Operationen steigt, ähnlich wie zum Beispiel beim Einsatz einer Luftwaffe, im Verbund mit anderen konventionellen Fähigkeiten. Den strategischen Planern von *Nitro Zeus* war unklar, wie lange die Wirkung der geplanten Cyber-Attacken andauern würde und wie resilient Irans Systeme waren. Um eine Nation dauerhaft elektronisch auszuschalten, müssten kontinuierlich Ressourcen aufgewendet werden.[45] Das war ein Grund, warum der Plan verworfen wurde.

Strategische OMCO sind ungeeignet für zwei zentrale militärische Ziele: die Entwaffnung gegnerischer Streitkräfte und die physische Besetzung eines Territoriums.

Zweitens muss immer ein Gegenschlag befürchtet werden. Die Angst vor Vergeltungsmaßnahmen gegen die eigene verwundbare kritische Infrastruktur ist — folgt man der Literatur — eine zentrale Erklärung dafür, warum großflächige strategische Cyber-Angriffe sehr selten ausgeführt werden.[46] Eine großangelegte strategische OMCO würde überdies völkerrechtlich höchstwahrscheinlich als Anwendung von Gewalt angesehen werden und somit vermutlich zu einem konventionellen Konflikt eskalieren. Darüber hinaus besteht das Risiko von Kollateralschäden und unbeabsichtigten Kaskadeneffekten. Im Fall von *Nitro Zeus* wäre zum Beispiel nicht klar gewesen, welche Strahlwirkung ein Ausfall iranischer Infrastruktur in der Region oder etwa auf globale Börsenkurse gehabt hätte. Gleiches gilt grundsätzlich auch bei konventionellen Angriffen.

44 Martin C. Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica, Cal.: RAND Corporation, 2009, S. 59, <https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf>.
45 Max Smeets, »The Strategic Promise of Offensive Cyber Operations«, in: *Strategic Studies Quarterly*, 12 (Herbst 2018), S. 90—113.
46 Brandon Valeriano / Ryan C. Maness, *Cyber War versus Cyber Realities. Cyber Conflict in the International System*, Oxford: Oxford University Press, 2015.

Drittens wächst mit der hohen Komplexität dieser Operationen auch die Unsicherheit über ihre Zuverlässigkeit. Strategische OMCO erfordern eine konzertierte und parallele Ausnutzung verschiedener Angriffsvektoren. Diese müssen im Vorfeld etabliert werden, indem etwa Netzwerkimplantate, also Schadsoftware mit verborgener Hintertür, in gegnerischen Systemen platziert werden (»preparation of the battlefield«). Diese Implantate können dann im Konfliktfall zeitgleich ausgenutzt werden. Sie können aber auch jederzeit vom Gegner entdeckt und somit nutzlos werden. Zudem verändern sich die Zielkonfigurationen permanent, wenn Updates eingespielt werden und Software ausgetauscht wird. Da Schadsoftware oft auf unbekannten 0-Day-Schwachstellen basiert, kommt es vor, dass mit einem Update des Zielsystems die Schwachstelle behoben und damit auch das darauf basierende Implantat wirkungslos wird. Daher muss permanent sichergestellt werden, dass eigene offensive Schadsoftware-Arsenale noch zur Zielkonfiguration des Gegners passen und nicht etwa wertlos geworden sind. Um die Angriffssoftware aktuell zu halten, müssen kontinuierlich Ressourcen aufgewendet werden. Lillian Ablon und Andy Bogart schätzen die Entwicklungszeit komplexer Malware auf mindestens 3 – 6 Monate, je nach Fähigkeitsniveau des Angreifers.[47] In einem strategischen Einsatz müssen Teams eingesetzt werden, die den Status der Implantate und der Schadsoftware dauernd verfolgen, um insbesondere zu erkennen, wie die konzipierten Angriffsvektoren miteinander verflochten oder voneinander abhängig sind. Müssen verschiedene Cyber-Angriffe etwa in einer bestimmten Reihenfolge stattfinden, verliert die Angriffskette ihre Wirkung, wenn am Anfang eine essentielle Schwachstelle beim Gegner behoben wurde. Das alles erfordert einen enormen logistischen Aufwand und vermutlich Hunderte verschiedener Cyber-Angriffsteams mit effizienter Organisationsführung. Kleinere Cyber-Mächte wie Deutschland werden so etwas allein wegen der dazu nötigen Manpower nicht stemmen können. Laut Sanger berichteten Insider, dass selbst die zahlreichen Hacker des US-CYBERCOM logistische Schwierigkeiten hatten, alle geheimen Implantate in iranischen Netzwerken aktuell zu halten, also sicherzustellen, dass diese weiterhin funktionierten.[48]

Viertens sind OMCO zielabhängig, was sie weniger flexibel macht als konventionelle Mittel und somit militärische Planungsprozesse durcheinanderbringen kann. OMCO müssen kontinuierlich und zeitaufwendig auf Zielkonfigurationen zugeschnitten werden, da sich die individuellen Konfigurationen, beispielsweise von Taliban-Computern oder russischen Systemen, unterscheiden. Die große Herausforderung, die damit verbunden ist, besteht nicht nur in der Sprachbarriere, sondern auch in unterschiedlichen Betriebssystemen, Softwarekonfigurationen und IT-Sicherheitsstandards. Hochwertige Ziele wie kritische Infrastrukturen und militärische Führungssysteme sind oft besonders gesichert und zum Beispiel nicht mit dem Internet verbunden (»air gap«). Das erfordert ein zeitintensives »Social-Engineering« oder gar das Einschleusen von Agenten, die die Schadsoftware händisch ins Ziel bringen.[49] Militärische Waffensysteme verfügen mitunter über eigens entwickelte und nicht auf dem freien Markt verfügbare Betriebssysteme. Cyber-Angriffe auf solche Ziele setzen seltenes Spezialwissen voraus.

Weil Cyber-Angriffe maßgeschneidert sein müssen, entsteht fast zwangsläufig eine Vorfeldverlagerung von OMCO in Friedenszeiten.

Durch das Erfordernis, dass Cyber-Angriffe maßgeschneidert sein müssen, entsteht fast zwangsläufig eine Vorfeldverlagerung von OMCO in Friedenszeiten, die sich bei zahlreichen Cyber-Mächten beobachten lässt: Um in einem militärischen Einsatz verfügbar zu sein, muss 0-Day-Malware im Vorfeld geschrieben und erfolgreich mittels Social-Engineering in ein Zielnetzwerk infiltriert werden. Andernfalls verringert sich der strategische Nutzen von OMCO als Mittel für Streitkräfte. Im Umkehrschluss stellt sich dadurch ein spezifisches Problem, das Kaltstartproblem: Findet

47 Lillian Ablon / Andy Bogart, *Zero Days, Thousands of Nights. The Life and Times of Zero-Day Vulnerabilities and Their Exploits*, Santa Monica, Cal.: RAND, 2017 (Research Report, RR-1751-RC), <www.rand.org/pubs/research_reports/RR1751.html>.

48 David Sanger / Mark Mazzetti, »U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict«, *New York Times* (online), 16.2.2016, <https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html>.

49 Mit Social Engineering werden Aktivitäten bezeichnet, die auf das Ausforschen sicherheitsrelevanter Daten durch menschliche Komponenten gerichtet sind. *Stuxnet* gelangte wohl über USB-Sticks, die von Agenten platziert wurden, in die gut gesicherten iranischen Atomanlagen.

keine Vorbereitung in Friedenszeiten statt, müssen OMCO-Tools erst mit dem Ausbruch eines Konflikts entwickelt werden, was deren Einsatz massiv verlangsamt. Daraus kann gefolgert werden, dass strategische OMCO nur in der Frühphase eines Konflikts wertvoll sein können, um beispielsweise Überraschungseffekte zu erzielen.[50] Bei nicht antizipierten Krisen dürfte das Tool nicht rechtzeitig einsatzbereit sein. Je länger Cyber-Konflikte andauern, desto mehr 0-Day-Schadsoftware wird verbrennen, das heißt entdeckt und durch Patches behoben werden. Ist diese »Verbrennungsrate« größer als die Reproduktionsrate eigener Entwicklerteams, werden Cyber-Arsenale irgendwann aufgebraucht sein.

Es gibt erhebliche Zweifel an den intendierten strategischen Effekten von OMCO, also an deren Wirksamkeit bei der Beeinflussung der Kosten-Nutzen-Kalküle des Gegners.

Fünftens gibt es auch erhebliche Zweifel an den intendierten strategischen Effekten von OMCO, also an deren Wirksamkeit bei der Beeinflussung der Kosten-Nutzen-Kalküle des Gegners.[51] Empirische Studien zeigen, dass mit strategischen Angriffen etwa auf zivile kritische Infrastrukturen, egal ob konventionell oder digital, fast nie das genuin militärische Ziel erreicht wird, den Widerstandswillen des Gegners zu brechen. Vielmehr werden diese Attacken als unrechtmäßig empfunden, was einen »Rally-around-the-flag«-Effekt erzeugt, der dazu führt, dass die Bevölkerung die Kriegsanstrengungen ihrer Regierung noch mehr unterstützt.[52] In Analogie dazu könnte dasselbe für eine OMCO gelten, die eine ganze Zielgesellschaft lahmlegt.[53]

Neben diesen Begrenzungen gibt es aber einen unbestreitbaren Vorteil der strategischen Cyber-Kriegsführung, nämlich eine weitere Option »short of war« auf dem Tisch zu haben, falls andere staatliche Machtmittel wie Diplomatie oder wirtschaftliche Sanktionen versagen. Max Smeets argumentiert, dass OMCO ähnlich wie verdeckte Operationen von Spezialeinheiten den Staatschefs eine alternative Handlungsoption bieten, die das Risiko einer Eskalation zu einem physischen Konflikt reduzieren kann.[54] Da die Urheberschafft bei Cyber-Angriffen häufig nur schwer zu bestimmen ist (Attributionsproblem), erlauben diese es den Initiatoren zudem, die Verantwortung dafür plausibel zu bestreiten. Oft sind Cyber-Operationen zudem eine kostengünstige Alternative zu militärischen Schlägen oder zum Einsatz von Spezialeinheiten. Die weitgehende Reversibilität der durch OMCO zugefügten Schäden könnte eine Option für eine humanere Kriegsführung sein. Der strategische Nutzen von OMCO ist also auch relativ zu sehen: Oftmals sind sie unter verschiedenen suboptimalen Handlungsalternativen die am wenigsten schlechte.

Operative OMCO

Im Kontext bewaffneter Konflikte werden Cyber-Fähigkeiten, anders als beim strategischen Cyber-Krieg, nicht als autonome (»Stand-alone«-) Komponente verstanden, mit deren Hilfe Kriege eigenständig gewonnen werden können, sondern als Ergänzung zu kinetischen, das heißt im engeren Sinne militärischen Mitteln.[55] Cyber-Angriffe richten sich hierbei gegen Ziele, die relevant für eine militärische Operation sind, also in der Regel gegen Kommando- und Leitstellensysteme von Streitkräften, oder gegen militärisches Gerät.[56]

Dank der Entwicklungen der letzten Jahre, zum Beispiel im Bereich der Vernetzung (»network centric warfare«) und Automatisierung, ist militärisches Gerät heutzutage ein komplexes System verschiedener Subsysteme. Der Eurofighter wird nicht durch

50 Nadiya Kostyuk / Yuri M. Zhukov, »Invisible Digital Front. Can Cyber Attacks Shape Battlefield Events?«, in: *Journal of Conflict Resolution*, 63 (2017) 2, S. 317 – 347.

51 Matthias Schulze, *Überschätzte Cyber-Abschreckung. Analyse der in der neuen US Cyber-Doktrin vorgesehenen Abschreckungspotenziale und Lehren für Deutschlands »aktive Cyberabwehr«*, Berlin: Stiftung Wissenschaft und Politik, 2019 (SWP-Aktuell 39/2019), <www.swp-berlin.org/publikation/ueberschaetzte-cyber-abschreckung/>.

52 Robert A. Pape, *Bombing to Win. Air Power and Coercion in War*, Ithaca, NY: Cornell University Press, 1996 (Cornell Studies in Political Economy).

53 Sean Lawson, »Beyond Cyber-Doom. Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats«, in: *Journal of Information Technology & Politics*, 10 (2013) 1, S. 86 – 103.

54 Max Smeets / Herbert S.Lin, »Offensive Cyber Capabilities: To What Ends?«, in: *10th International Conference on Cyber Conflict CyConX: Maximising Effects*, Tallinn 2018, S. 55 – 71.

55 Gartzke, »The Myth of Cyberwar« [wie Fn. 43].

56 Smeets, »The Strategic Promise of Offensive Cyber Operations« [wie Fn. 45], S. 94.

Fallstudie *Operation Orchard* 2007

Über die *Operation Orchard* sind nur wenige Details bekannt. Mutmaßlich israelische Hacker sabotierten am 6. September 2007 ein syrisches Flugabwehrradar. Sie manipulierten den Datenlink zwischen Radar und Computerbildschirmen mittels einer Schadsoftware.[a] Das führte dazu, dass auf den Bildschirmen der syrischen Flugüberwachung nicht zu erkennen war, dass israelische F-15-Jets in den syrischen Luftraum eindrangen und per Luftangriff das Atomtestgelände in Deir el-Zor im Norden Syriens zerstörten. Sowohl Israel als auch Syrien verneinten, dass das Ereignis je stattgefunden habe. Berichten zufolge wurde zunächst eine ISR-Schadsoftware per Hand auf dem Notebook eines syrischen Atomwissenschaftlers installiert, als dieser sich in einem Londoner Hotel aufhielt.[b] Dies könnte der Ausgangspunkt für ein tiefes Eindringen in syrische Verteidigungsnetzwerke gewesen sein. Bereits diese eher niedrigschwellige Operation wird von einigen Völkerrechtlern als Verstoß gegen das Gewaltverbot interpretiert.[c]

a Fred M. Kaplan, *Dark Territory. The Secret History of Cyberwar*, New York u.a., 2016, S. 118.
b Kim Zetter, »Mossad Hacked Syrian Official's Computer before Bombing Mysterious Facility«, *Wired* (online), 11.3.2009, <https://www.wired.com/2009/11/mossad-hack/>.
c Andrew Garwood-Gowers, »Israel's Airstrike on Syria's Al-Kibar Facility: A Test Case for the Doctrine of Preemptive Self-Defence?«, in: *Journal of Conflict and Security Law*, 16 (2011) 2, S. 263–291.

einen zentralen Computer, sondern durch einen Verbund verschiedener Systeme gesteuert, die für unterschiedliche Aspekte des Flugzeugs zuständig sind, etwa die Schubdüsen, die Lebenserhaltung des Piloten oder Waffenleitsysteme. All diese Funktionen werden mittels Software und teils mittels kommerziell verfügbarer industrieller Steuerungschips gelenkt, die voller Sicherheitslücken und somit verwundbar gegenüber OMCO sind. Militärisches Gerät verfügt zudem über zahlreiche Schnittstellen, zum Beispiel Wartungsports, Kommunikations-, GPS-, oder Datenverbindungen, die sie mit militärischen Netzwerken oder bisweilen – zum Zweck der Fernwartung – mit den Herstellern verbinden. Über diese Schnittstellen sind Waffensysteme angreifbar. Da militärisches Gerät oft jahrzehntelang im Einsatz ist und der IT-Sicherheit bis vor wenigen Jahren in Beschaffungsprozessen keine Priorität zugemessen wurde, gibt es zahlreiche ältere Waffensysteme, die ein sehr schlechtes IT-Sicherheitsniveau aufweisen dürften. Das US Government Accountability Office (GAO) führte beispielsweise im Jahr 2018 ein Audit aller US-Beschaffungsprogramme des Pentagons durch und fand nahezu in allen modernen Waffensystemen missionskritische IT-Sicherheitsschwachstellen, die gegnerische Cyber-Angreifer mit geringem Kompetenzniveau und frei verfügbaren Angriffstools hätten ausnutzen können.[57] Zu den gängigsten Schwächen, auf die das GAO stieß, zählen Standardpasswörter, fehlende Updates und fehlende Verschlüsselung.

Da IT-gesteuerte Waffensysteme, militärische Kommunikationsnetzwerke, Hauptquartiere und weltweit verteilte Kommunikationsleitstellen eine recht große Angriffsfläche bieten, denken militärische Planer natürlich darüber nach, diese mittels OMCO lahmzulegen. Vorbereitende Cyber-Spionageangriffe gegen militärische Hauptquartiere, Verteidigungsministerien und Hersteller von Waffensystemen sind mittlerweile die Norm. Daher gibt es im Gegensatz zur strategischen Ebene jede Menge Beispiele für den operativen Einsatz von OMCO in bewaffneten Konflikten.

Die mutmaßlich von Israel im Jahr 2007 lancierte *Operation Orchard* ist ein Beispiel für die erfolgreiche sequentielle Nutzung von Cyber-Fähigkeiten als »Enabler« für kinetische Operationen, aber auch für den Einsatz bei einem Erstschlag.

Cyber-Mittel und konventionell-militärische Mittel erfolgreich korrelierend einzusetzen (»jointness«), ist eine zentrale Herausforderung für Cyber-Mächte, da sich die Synchronizität nicht leicht herstellen lässt. (Gleiches gilt im Übrigen grundsätzlich auch für die Integration verschiedener konventioneller Teilstreitkräfte.) Eine Studie von Kostyuk und Schukow über den Einsatz von Cyber- und kinetischen Militäroperationen in Syrien (2013) und in der Ostukraine (ab 2014) zeigt, dass das Timing bei synchronen Operationen oft nicht funktioniert. Konventionelle Angriffe und disruptive Cyber-Operationen wurden in beiden Konflikten weitgehend getrennt voneinander durchgeführt, ohne dass es zu gemeinsamen Effekten oder einer strategischen Wechselwirkung kam.[58] Russland

57 United States Government Accountability Office, *Weapon Systems Cybersecurity. DOD Just Beginnung to Grapple with Scale of Vulnerabilities*, Washington, D.C., Oktober 2018 (GAO-19-128), <https://www.gao.gov/products/GAO-19-128>.
58 Nadiya Kostyuik / Scott Power / Matt Skach, »Determinants of the Cyber Escalation Ladder«, in: *The Cyber Defense Review*, 3 (2018) 1, S. 123–134.

Fallstudie Georgien 2008

Russische Cyber-Operationen sind ein Beispiel für die parallele Nutzung von OMCO durch konventionelle Streitkräfte. Belege für dieses Vorgehen liefern der Krieg in Georgien 2008 und der Konflikt im Osten der Ukraine (seit 2014). Die militärische Eskalation des Konflikts in Georgien begann am 7. August 2008 im Zusammenhang mit einem Streit in Südossetien. Bereits drei Wochen zuvor waren die Websites der georgischen Regierung, des Finanzsektors und Kommunikationsplattformen von einfachen Distributed-Denial-of-Service-Angriffen (DDoS) betroffen. Diese Aktion war aber nur die Generalprobe für eine weitere Welle von DDoS-Attacken, die gleichzeitig mit dem Einmarsch der russischen Kampftruppen durchgeführt wurden. Diesmal war es das Ziel, die georgische Kommunikation mit der Außenwelt zu beeinträchtigen. In der georgischen Stadt Gori wurden unter anderem lokale Nachrichtenseiten durch DDoS-Angriffe kurz vor dem Eintreffen russischer Flugzeuge in der Stadt lahmgelegt.[a] Andere Cyber-Attacken richteten sich gegen georgische Websites, die verunstaltet wurden, um Chaos und Unsicherheit zu verbreiten. Kritische Infrastrukturen wurden jedoch nicht angegriffen. Die Komplexität der Angriffe kann als gering bezeichnet werden.

a David Hollis, »Cyberwar Case Study: Georgia 2008«, in: *Small Wars Journal*, 2011, <https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008>.

ist allerdings bekannt dafür, bei Cyber-Angriffen auch auf Drittakteure wie patriotische Hacker oder auf angeheuerte Cyber-Söldner zu setzen. Solche Proxy-Akteure sind vermutlich schwieriger zu steuern und zu einem koinzidenten Handeln zu bewegen als militärische Hacker in einer klaren Kommandokette.[59] James Lewis zieht daher für diesen Fall das Fazit, dass russische OMCO in der Ukraine über einen anfänglichen Überraschungseffekt hinaus keine taktischen oder operativen militärischen Effekte erzielt haben.[60] Allerdings ist anzunehmen, dass durch beständiges Üben und Simulieren die Synchronizität in Zukunft verbessert werden kann.

Zudem kann argumentiert werden, dass die russischen Cyber-Operationen in der Ostukraine vorwiegend auf psychologische Aspekte wie die Demoralisierung ukrainischer Soldaten und auf ISR-Zwecke abzielten. Schlagzeilen machte eine Schadsoftware, die 2016 auf den Smartphones ukrainischer Artilleriesoldaten gefunden wurde. Die Schadsoftware war in einer mobilen Applikation für die Zielführung von D-30-Howitzer-Artilleriestellungen eingebettet und übertrug die Geoposition dieser Artillerie. Die als »X-Agent« bezeichnete Schadsoftware wurde bereits ein Jahr vor der Eskalation entwickelt. Laut der Firma *Crowdstrike* sind bis 2017 zwischen 15 und 20 Prozent der ukrainischen D-30-Howitzer in Kampfeinsätzen vernichtet worden. Wie viele Verluste davon auf die Schadsoftware und wie viele auf eher traditionelle Aufklärung wie Drohnen zurückzuführen sind, ist kaum nachweisbar.[61]

Durch erfolgreiche Cyber-Angriffe sinkt das Vertrauen der Nutzer in die Authentizität, Integrität und Verfügbarkeit von Daten und Systemen.

Laut Erica Borghard und Shawn Lonergan eignen sich operative OMCO durchaus für Zermürbungsstrategien.[62] Mit offensiven Cyber-Operationen könnten gegnerische Kommandoketten so gestört werden, dass sich Nachrichten nicht mehr übermitteln lassen. Durch erfolgreiche Cyber-Angriffe sinkt das Vertrauen der Nutzer in die Authentizität, Integrität und Verfügbarkeit von Daten und Systemen. Wenn die Gefahr besteht, dass ein Gegner im eigenen Netzwerk mithört, werden dort keine sensiblen Informationen mehr eingegeben. Folglich müssen diese auf Wegen übermittelt werden, die in der Regel kostenintensiver sind, und die gesamte Operation wird langsamer. Diese psychologische Wirkung kann ein sinnvolles Einsatzziel sein. Mit Cyber-Angriffen können zudem die Verlegung und Logistik von Militärgerät erschwert und behindert werden, zum Beispiel der Transport von Panzern an ihre Zielorte.

59 Tim Maurer, *Cyber Mercenaries. The State, Hackers, and Power*, Cambridge: Cambridge University Press, 2017, S. 84ff.
60 Lewis, »›Compelling Opponents to Our Will‹« [wie Fn. 41].
61 »Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units«, *Crowdstrike* (online), 23.3.2017, <https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf>.
62 Erica D. Borghard / Shawn W. Lonergan, »The Logic of Coercion in Cyberspace«, in: *Security Studies*, 26 (2017) 3, S. 452 – 481 (474).

Fallstudie *Glowing Symphony* 2016

Eine verhältnismäßig gut dokumentierte OMCO ist die Operation *Glowing Symphony*, die sich gegen die digitalen Aktivitäten des ISIS[a] richtete. Zu diesen Aktivitäten zählten im Wesentlichen die Rekrutierung von Anhängern in sozialen Netzwerken, das Verbreiten von digitalen Propagandavideos und Memes, die interne Kommunikation und die Steuerung finanzieller Mittel. Das Ziel der OMCO war, die professionellen Online-Propagandaaktivitäten des IS zu stören, zu verlangsamen oder ganz zu unterbinden. Ferner sollte das interne Kommunikationsnetzwerk ausspioniert werden (ISR), um zum Vorteil der Koalitionsbodentruppen Informationen, etwa über die Identität von Administratoren und die Geoposition von ISIS-Kämpfern, zu gewinnen.[b]

Im November 2016, also gut ein Jahr nach Beginn der konventionellen Operation, begann US-CYBERCOM mit disruptiven Angriffen wie etwa dem Löschen bzw. Manipulieren von Servern, Social-Media-Accounts oder Bitcoin-Wallets. Schadsoftware wurde vorwiegend über eigens vorbereitete Phishing-Mails verteilt.[c] Die Operation hatte neben den disruptiven Effekten auch eine InfoOP-Komponente: Der Gegner sollte durch die Störung und Schwächung seiner digitalen Ressourcen frustriert und zermürbt werden. Zu diesem Zweck wurden ISIS-Rechner und Internetverbindungen verlangsamt, künstlich Fehlermeldungen generiert, Link-Adressen auf ISIS-Websites verändert, so dass sie ins Leere leiteten, und Passwörter von Administratoren geändert, so dass diese nicht mehr auf ihre Accounts zugreifen konnten.

a Islamischer Staat im Irak und in Syrien.
b Shannon Vavra, »U.S. Cyber-Offensive against ISIS Continues, and Eyes Are Now on Afghanistan, General Says«, *Cyberscoop* (online), 17.9.2019, <https://www.cyberscoop.com/isis-jtf-ares-cyber-offensive-afghanistan/>.
c Dina Temple-Raston, »How the U.S. Hacked ISIS«, *National Public Radio* (online), 26.9.2019, <https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis> (Zugriff am 11.6.2020).

Die Operation *Glowing Symphony* wird in internen Dokumenten als »die komplexeste offensive Cyberspace-Operation, die US-CYBERCOM je durchgeführt hat«, bezeichnet.[63] Die Cyber-Offensive, so erfolgreich sie auch war, bietet indes zahlreiche Erkenntnisse zu operativen Hindernissen. Erstens war die interne Koordination zwischen US-CYBERCOM, NSA, den anderen Teilstreitkräften und den Koalitionspartnern (Australien und Großbritannien, die ebenso OMCO gegen ISIS starteten) enorm komplex, was die OMCO dramatisch verlangsamte.[64] Eine Schwierigkeit dabei war, dass physisches und digitales Einsatzgebiet nicht korrelierten: ISIS speicherte seine Online-Propaganda weltweit in über 35 Ländern, teilweise auf kommerziellen Systemen, die auch für kritische Infrastrukturen relevant waren.[65] Ein einfaches Abschalten dieser Systeme hätte unübersehbare Kollateralschäden verursachen können. Insofern mussten die Aktivitäten mit allen beteiligten Ländern diskutiert, synchronisiert und auf ihre Folgeeffekte hin durchleuchtet werden.[66]

Zweitens gab es Zielkonflikte zwischen dem Nachrichtendienst NSA und den militärischen Planern. Die NSA wollte im Gegensatz zur Militärbehörde US-CYBERCOM Server nicht abschalten, um sie weiterhin überwachen zu können. Der Standpunkt des Nachrichtendienstes begründet sich mit dem begrenzten Lebenszyklus und dem Erfordernis der Zielanpassung von Schadsoftware. Mit dem Auslösen disruptiver Effekte steigt das Risiko, dass Schadsoftware und Hintertürimplantate, die mit großem Aufwand konfiguriert wurden, entdeckt werden und somit »verbrennen« — für die Dienste gleichbedeutend mit einem Zugangsverlust.

Drittens war ISIS ein dynamischer und vor allem resilienter Gegner, der die träge US-CYBERCOM-Bürokratie immer wieder ausmanövrierte. Anfangs fanden die US-CYBERCOM-OMCO nur episodisch und nicht kontinuierlich statt. Propaganda wurde zwar von Servern gelöscht, tauchte dann aber blitzschnell auf anderen Servern wieder auf, weil ISIS sich auf redundante Infrastrukturen stützen konnte.

63 Michael Martelle, »USCYBERCOM after Action Assessments of Operation GLOWING SYMPHONY«, *National Security Archive* (online), 21.1.2020, <https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony> (Zugriff am 11.6.2020).

64 Shannon Vavra, »Top Secret Documents Show Cyber Command's Growing Pains in Its Mission against ISIS«, *Cyberscoop* (online), 21.1.2020, <www.cyberscoop.com/cyber-command-pentagon-counter-isis-glowing-symphony-foia/> (Zugriff am 11.6.2020).
65 Ellen Nakashima, »U.S. Military Cyber Operation to Attack ISIS Last Year Sparked Heated Debate over Alerting Allies«, *Washington Post* (online), 8.5.2017, <https://wapo.st/31yswQP>.
66 Ebd.

»Ich war weitgehend enttäuscht über die Effektivität des Cyber Command gegen ISIS. Es hat nie wirklich effektive Cyber-Waffen oder -Techniken hervorgebracht« (Ashton Carter)

So fällt die Beurteilung der Operation *Glowing Symphony* gemischt aus: Nach anfänglichen Startschwierigkeiten ging die Online-Aktivität des IS tatsächlich zurück. Ob dies auf die Cyber-Angriffe oder nicht doch auf die physische Zurückdrängung des IS zurückzuführen ist, bleibt unklar.[67] Die selbstgesteckten Ziele wurden auf jeden Fall erreicht: Die Social-Media-Aktivitäten des IS wurden verlangsamt, zahlreiche Accounts gesperrt und auch eine ganze Menge Online-Videomaterial entfernt.[68] Verteidigungsminister Asthon Carter jedoch zeigte sich im Nachgang vom tatsächlichen Nutzen der OMCO unbefriedigt: »Ich war weitgehend enttäuscht über die Effektivität des Cyber Command gegen ISIS. Es hat nie wirklich effektive Cyber-Waffen oder -Techniken hervorgebracht. Wenn US-CYBERCOM etwas Nützliches produzierte, neigten die Geheimdienste dazu, die Verwendung zu verzögern oder zu verhindern, indem sie behaupteten, Cyber-Operationen würden das Sammeln von Informationen behindern.«[69]

Dies deutet darauf hin, dass operative Cyber-Fähigkeiten (derzeit) ein nur begrenzt wirksames militärisches Instrument sind. Das kann sich in Zukunft ändern, etwa durch beständiges Üben von Einsätzen oder dadurch, dass zukünftige Gegner in höherem Maße technisiert sind. Allerdings sind zahlreiche andere traditionelle Mittel wie Panzer oder Fregatten gegen agile, global-agierende Terrornetzwerke ebenso nur bedingt tauglich.

Taktische OMCO

Das Gros der Waffeneinsätze in Konflikten findet auf der taktischen Ebene, also der Ebene der Soldaten und Soldatinnen im Feld statt. Gefechte auf der taktischen Ebene dienen dazu, die übergeordneten Ziele einer Operation zu erreichen. Auch OMCO können in die taktische Planung integriert werden, wenngleich diese Art Cyber-Operation bisher vergleichsweise am wenigsten erforscht ist.

Andrew Metcalf und Christopher Barber definieren »tactical cyber« als »Cyber Operationen innerhalb und außerhalb eigener Netzwerke, die im Kontext eines traditionellen kinetischen Schlachtfelds durchgeführt werden, wobei die Autorisierung, die »Deconfliction« [siehe dazu im Folgenden] und die Kontrolle über die spezifische Operation auf Bataillonsebene oder niedriger stattfinden«.[70] Dass hier die Kommandoebene genannt wird, dient der Abgrenzung zu den operativen und strategischen Cyber-Fähigkeiten, über die auf höheren Ebenen entschieden wird. »Deconfliction« lässt sich mit einem Wort kaum ins Deutsche übersetzen. Gemeint ist aber das Überwinden der möglicherweise widerstreitenden Interessen und Zuständigkeiten der verschiedenen Kommandoebenen oder auch Nachrichtendienste, also jener spannungsgeladenen Situation, die sich beispielsweise bei *Glowing Symphony* eingestellt hat. In den meisten Cyber-Nationen wird der Einsatz offensiver Fähigkeiten auf der strategischen Ebene entschieden, das heißt weit oben in der militärischen Befehlskette. Strategische Cyber-Fähigkeiten können jedoch nicht einfach für den taktischen Einsatz auf den unteren Ebenen der Befehlskette umgewandelt werden, da der Nutzungskontext anders ist.[71]

Aufgrund der längeren Entwicklungszyklen ist es schwer, Schadsoftware in taktische Planungsprozesse zu integrieren. Zudem ist es sinnlos, große Geldsummen in eine verdeckte taktische Cyber-Fähigkeit zu investieren, wenn sie bereits in der ersten Mission aufgedeckt und damit unwirksam wird. Vertraulichkeitserfordernisse und taktischer Einsatz standen schon immer miteinander im Konflikt, da in Kampfsituationen beispielsweise die Ausrüstung vom Gegner erbeutet werden kann.

Taktische OMCO unterliegen aber noch anderen Beschränkungen, was erklärt, warum sie nur selten eingesetzt werden. Im Gegensatz zu Mikrodrohnen, Personal Digital Assistants, Anti-IED-Geräten und anderen digitalen Hilfsmitteln des »Infanteristen der

67 Martelle, »USCYBERCOM after Action Assessments of Operation GLOWING SYMPHONY« [wie Fn. 63].

68 Shannon Vavra, »U.S. Cyber-Offensive against ISIS Continues, and Eyes Are Now on Afghanistan, General Says«, *Cyberscoop* (online), 17.9.2019, <www.cyberscoop.com/isis-jtf-ares-cyber-offensive-afghanistan/>.

69 Ash Carter, *A Lasting Defeat: The Campaign to Destroy ISIS*, Boston: Harvard Kennedy Law School. Belfer Center for Science and International Affairs, Oktober 2017, S. 33.

70 Andrew O. Metcalf / Christopher Barber, »Tactical Cyber: How to Move Forward?«, *Small Wars Journal* (online), 14.9.2014, <https://smallwarsjournal.com/jrnl/art/tactical-cyber-how-to-move-forward> (Übersetzung durch den Autor).

71 Ebd.

Fallstudie Irak 2007

Dem Journalisten Shane Harris zufolge hatte die NSA seit 2004 umfassenden, physischen Zugang zum »Backbone«, also zu den zentralen Rechenzentren der irakischen Telefon- und Internetanbieter. Sie war daher in der Lage, die Metadaten irakischer Mobiltelefone und den Internet-Datenverkehr zu lesen. Diese Informationen waren nützlich, um die Urheber hinter improvisierten Sprengsätzen (IED) zu verfolgen, die 2007 für US-Patrouillen eine große Belästigung darstellten. Die NSA korrelierte die Telefon-Metadaten mit geografischen Karten und konnte so die Geoposition der Mobiltelefone bestimmen, die zum Auslösen der IED verwendet wurden. Die NSA konnte einige davon aus der Ferne zerstören oder die Position von Aufständischen in der Nähe ermitteln. Dies ist ein Beispiel für taktische ISR-Fähigkeiten.[a]

Die zweite Komponente der Operation betraf den Einsatz von Malware gegen die Computersysteme der Aufständischen. Zum einen wurden in einer großangelegten Aktion manipulierte Phishing-E-Mails an irakische Ziele verteilt, potentiell auch an Zivilisten. Zum anderen wurden gezielt Computer über USB-Sticks infiziert, die von taktischen Cyber-Einheiten in gegnerische Stützpunkte eingebracht wurden. Ziel war es, das gegnerische Informations- und Kommunikationsnetzwerk Obelisk, eine Art al-Qaida-Intranet, zu kompromittieren.[b]

Die dritte Komponente bestand aus Informationsoperationen gegen Aufständische. Über ihren Zugang zum irakischen Telefonnetz schickten die US-Truppen gefälschte Textnachrichten an die Aufständischen, um sie zu demoralisieren oder ihnen Fallen zu stellen. So wurden beispielsweise Personen zu Treffen gelockt, bei denen sie dann gefangengenommen wurde. Malware wurde auch eingesetzt, um Personen ausfindig zu machen, die Propagandavideos über Internet-Cafés hochgeladen hatten.

a Shane Harris, *@War. The Rise of the Military-Internet Complex*, Boston/New York: Mariner Books, 2015, S. 3ff.
b Ebd., S. 31.

Zukunft« sind taktische Cyber-Fähigkeiten schwer zu standardisieren, zu verpacken und mitzuführen. Die Anforderung, OMCO auf Ziele zuschneidern zu müssen, steht im Widerspruch zu den Anforderungen der Truppen im Feld. Diese brauchen Werkzeuge, die wiederholt und zuverlässig gegen alle möglichen Ziele einsetzbar sind. Ein Anti-IED-Gerät, das nur gegen eine bestimmte Art von Mobiltelefon funktioniert, ist weniger wertvoll als eines, das gegen alle Arten von Mobiltelefonen funktioniert. Aufgrund dieser Eigenschaften von Cyber-Fähigkeiten sind sie für taktische Einheiten weniger geeignet.[72]

Wie bei allen Cyber-Angrifftools sind Kollateralschäden im Voraus nur schwer vorhersehbar. So ist es beispielsweise denkbar, dass eine OMCO, die sich gegen eine smarte Internet-of-Things-(IoT-)Überwachungskamera in einem Gebäude richtet, eskaliert, weil deren Services in der Cloud gehostet werden. Zahlreiche billige IoT-Kameras zum Beispiel speichern ihre Daten auf chinesischen Servern.[73] Um diese Kameras zu hacken, könnte sich eine Cyber-Operation unter Umständen auch gegen Server auf chinesischem Territorium richten. Eine OMCO gegen solch ein System kann also Cyber-Angriffe gegen unbeteiligte Drittstaaten implizieren. Darüber hinaus besteht immer die Gefahr, dass die zivile Infrastruktur unbeabsichtigt beeinträchtigt wird.[74] Das grundlegende Problem bei all diesen Operationen ist, dass der Cyberspace nicht mit der Geografie des Schlachtfelds vor Ort übereinstimmt.[75] Der taktische Einsatz kann daher strategische Auswirkungen haben. Das ist auch der Grund, warum die strategische Kommandoebene die Entscheidung über den taktischen OMCO-Einsatz ungern an die Bataillonsebene abgibt.

Taktische Cyber-Operationen im Feld sind nur dann sinnvoll, wenn eine räumliche Nähe gegeben ist, wie etwa in urbanen Kontexten.

Schließlich zeigen die Erfahrungen in Afghanistan und im Irak, dass die Technologie in schwierigen Umgebungen — wie weiten Landschaften und Wüsten — tendenziell versagt. Damit taktische OMCO funktionieren, muss eine Datenverbindung mit ausreichender Bandbreite bestehen. Computer brauchen Strom. Diese Voraussetzungen können in Kampfsituationen nicht zuverlässig erfüllt werden, insbesondere wenn der Gegner über Mittel elektronischer Kriegsführung verfügt. Für Cyber-Operationen im Feld ist in der Regel eine gewisse Nähe zum Ziel erforderlich. Ein

72 Isaac Porche u.a., *Tactical Cyber. Building a Strategy for Cyber Support to Corps and Below*, Santa Monica, Cal.: RAND, 2017 (Research Report, RR-1600-A), S. 47ff, <https://www.rand.org/pubs/research_reports/RR1600.html>.
73 Maya Shwayder, »Yes, China Is Probably Watching Us through Our IoT Devices«, *Digital Trends* (online), 6.2.2020, <https://www.digitaltrends.com/news/china-spying-iot-devices/> (Zugriff am 19.5.2020).
74 Porche u.a., *Tactical Cyber* [wie Fn. 72], S. 47ff.
75 Metcalf/Barber, *Tactical Cyber* [wie Fn. 70].

gegnerisches WLAN kann nur innerhalb des Funkwellenbereichs gehackt werden. Taktische Cyber-Operationen im Feld sind daher nur dann sinnvoll, wenn eine räumliche Nähe gegeben ist, wie etwa in urbanen Kontexten. In weiten, ländlichen Regionen taugt das Mittel vermutlich weniger.

Zusammenfassung und Typologie verschiedener OMCO

Die Analyse hat gezeigt, dass Cyber-Operation nicht gleich Cyber-Operation ist. Es gibt eine erhebliche Bandbreite beim Umfang und bei der Intensität von OMCO (siehe Grafik 3, S. 30f). Dadurch haben die verschiedenen Operationen zum Teil sehr unterschiedliche rechtliche, technische und operative Vorbedingungen, die erfüllt sein müssen, damit sie erfolgreich sein können.

Cyber-Angreifer sollten sich sehr sicher sein, dass ihr Vorstoß tatsächlich wirkt und keine unbeabsichtigten Kollateralschäden entstehen.

Am unteren Ende der Umfangs- und Intensitätsdimension finden sich sehr zielgenaue OMCO, mit temporär, regional und in ihrer Wirkintensität begrenzten Effekten, wie *Operation Orchard*. Solche disruptiven Störangriffe zum Lahmlegen einzelner, für ein Missionsziel relevanter Systeme wie etwa Radaranlagen oder ISIS-Propagandaserver machen die Mehrzahl der analysierten Fälle aus. Der Einsatz ist vergleichbar mit der Verwendung elektromagnetischer Störsender und dürfte daher ähnliche operative und rechtliche Implikationen haben. Da derartige Operationen nur wenige Ziele betreffen, sind sie leichter — auch von kleineren Angriffsteams — durchzuführen. Die Schwierigkeiten bei dieser Art Attacke bestehen darin, das richtige Timing zu finden, etwa wenn die Cyber-Operation sequenziell bzw. als »Enabler« für eine konventionelle Operation genutzt werden soll. Cyber-Angreifer sollten sich sehr sicher sein, dass ihr Vorstoß tatsächlich wirkt, keine unbeabsichtigten Kollateralschäden entstehen und nachgelagerte Missionen nicht durch ein Versagen oder Fehler gefährdet werden. Das erfordert gute Informationen über Zielsysteme sowie einiges an sorgfältiger Vorbereitung, um die Schadsoftware unter realen bzw. bestmöglichen Bedingungen zu testen. Wie bei konventionellen Angriffen muss auf jeden Fall eine Abschätzung potentieller Folgen stattfinden.

Am oberen Ende der Umfangs- und Intensitätsskala stehen sehr breite strategische Operationen, die Hunderte, teils willkürliche militärische und zivile Ziele mit unterschiedlichen Schutzniveaus treffen. *Nitro Zeus* ist hier das extremste Beispiel, aber auch die Cyber-Operationen Russlands in der Ukraine hatten globale Effekte, insbesondere in Form der *Not-Petya*-Schadsoftware, die weltweit Systeme lahmlegte und Millionen von Kosten verursacht hat.[76] *Not-Petya* sollte eigentlich nur ukrainische Ziele treffen, verbreitete sich aber global — ein Beleg für das immanente Risiko von Kollateralschäden. Solche Operationen haben eine enorme Komplexität und sind logistisch nicht von jeder Cyber-Macht zu stemmen. Teil strategischer OMCO wie *Nitro Zeus* sind in der Regel sehr intensive und invasive Sabotageangriffe auf kritische Infrastrukturen wie Energieversorger. Auch russische Hacker legten in der Ukraine bereits zwei Mal Stromkraftwerke lahm.[77] Solche Angriffe gelten als extrem gefährlich, da dort konkret Menschenleben aufs Spiel gesetzt werden. Deshalb beinhalten sie ein enormes Eskalationsrisiko. Zudem sind diese Operationen extrem komplex, denn in ihrem Verlauf müssen in der Regel mehrere unbekannte 0-Day-Schwachstellen ausgenutzt werden, um unbemerkt in Systeme mit hohem Schutzniveau einzudringen. Dazu werden arbeitsteilig operierende Angriffsteams mit hohen Fähigkeiten gebraucht, genauso wie sehr gute geheimdienstliche Zugänge, um interne Informationen über industrielle Steuerungsanlagen zu erhalten. Das heißt, diese Operationen werden für zweitklassige oder mit geringen Ressourcen ausgestattete Cyber-Angreifer kaum durchführbar sein. Gleiches gilt auch für strategische Informationsoperationen, wie sie Russland ebenfalls in der Ukraine lanciert. Auch für diese Zwecke sind ganze Einheiten von Linguisten, Regionalexperten und Social-Media-Teams notwendig.

Die Analyse der verschiedenen OMCO-Typen zeigt den Nutzen und die Begrenzungen dieser Operationen. Der größte Nutzen besteht wohl in »Intelligence, Surveillance and Reconnaissance«, also in der Generie-

76 Andy Greenberg, »The Untold Story of NotPetya, the Most Devastating Cyberattack in History«, *Wired* (online), 22.8.2018, <www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.

77 Andy Greenberg, »How an Entire Nation Became Russia's Test Lab for Cyberwar«, *Wired* (online), 20.6.2017, <https://www.wired.com/story/russian-hackers-attack-ukraine/> (Zugriff am 11.6.2020).

rung wichtiger Informationen, etwa über Truppenpositionen und -bewegungen, über interne Kommunikationsnetze und somit die operative Planung des Gegners. ISR-OMCO gegen staatliche Gegner scheinen weniger kompliziert zu sein, da klar ist, welche Akteure man angreift. Beim Einsatz gegen Aufständische sind zunächst aufwendige Vorfeldanalysen nötig, umdie Kombattanten, die man schwächen will, überhaupt von unbeteiligten Zivilisten zu scheiden.

Zweitens ist der Zeitpunkt der Nutzung einer Cyber-Fähigkeit von Bedeutung. Es scheint, dass die Anwendung in der Form eines Erstschlags in einem Konflikt leichter zu bewerkstelligen ist als das Durchführen einer kontinuierlichen Cyber-Operation. In den meisten Fällen, in denen sie Teil einer operativen Planung waren (*Orchard*, Georgien, *Nitro Zeus*), wurden OMCO in der Frühphase eines Konflikts eingesetzt. Allerdings sind singuläre Erstschläge gegen resiliente Gegner wirkungslos, wenn diese die Fähigkeit haben, ihre Systeme schnell wieder hochzufahren oder auf Alternativen auszuweichen (Cyber-Resilienz). Generell gilt: Je mehr Vorbereitungszeit vorhanden ist, desto wahrscheinlicher ist der Erfolg einer Cyber-Operation.

Der dritte Aspekt ist die Frage, wie schwer die Mission durchzuführen ist. Hier spielen mehrere Faktoren eine Rolle, etwa die Verfügbarkeit von Informationen, die benötigt werden, um Zugang zu allen schwer zu treffenden Zielen zu erhalten. Strategische OMCO scheinen leichter durchführbar zu sein, da sich mit ihnen weniger gut gesicherte zivile Ziele angreifen lassen und sie in der Masse für Chaos sorgen können. Operative OMCO gegen gut gesicherte militärische Ziele erfordern offenbar einen größeren Aufwand, wobei dies immer auf den Einzelfall ankommt. OMCO werden riskanter und weniger leicht ausführbar werden, wenn es keine zuverlässigen Informationen über die Ziele gibt.

OMCO werden häufig bereits in Friedenszeiten entwickelt, um im Konfliktfall einsatzbereit zu sein. Andernfalls droht ein Kaltstartproblem.

Je besser die Cyber-Abwehr des Verteidigers, desto schwieriger ist es, OMCO durchzuführen, und desto länger wird die Vorbereitungszeit. Alle untersuchten Operationen hatten eine lange Vorlaufzeit von Monaten bis Jahren. Damit bestätigt sich empirisch die These der Vorfeldverlagerung: OMCO werden häufig bereits in Friedenszeiten entwickelt, um im Konfliktfall einsatzbereit zu sein. Andernfalls droht ein Kaltstartproblem. Auch die Anzahl der potentiellen Ziele spielt eine Rolle. Gegen wenig digitalisierte Gegner sind Cyber-Fähigkeiten nutzlos. Gegen Hochtechnologieziele sind sie sinnvoller, denn diese öffnen in der Regel die Flanke für mehrere Angriffsvektoren.

Der letzte Aspekt ist die OMCO-Fähigkeit der eigenen Streitkräfte. Diese ist wiederum eine Funktion der Größe und der Organisation eigener Cyber-Kräfte. In allen analysierten Fällen verfügten die Angreifer sowohl über recht große als auch extrem kompetente Angriffsteams. Israel, die USA und Russland gehören neben China zu den besten Cyber-Angreifern, da sie zum Beispiel regelmäßig unbekannte 0-Day-Schwachstellen in ihren Attacken einsetzen. Dies gilt als die Königsdisziplin im Cyber-Operationsmetier, denn die Vorbereitung solcher Offensiven übersteigt die Fähigkeiten kleinerer Cyber-Mächte mit geringerem Niveau oft. Allerdings sind größere Angreiferteams potentiell schwieriger zu synchronisieren als kleinere. Kleinere Teams sind aller Erkenntnis nach in der Anzahl der Ziele, die sie gleichzeitig oder über einen längeren Zeitraum durchdringen können, eingeschränkter. Größere Teams können offenbar in kürzerer Zeit größere Bestände an Malware produzieren. Das hängt indes auch davon ab, wie die verschiedenen Cyber-Teams, Bug-Hunter, Malware-Coder, Infrastrukturmanager, Linguisten und Analysten zusammenarbeiten. Darüber hinaus spielt der Grad der Integration der Cyber-Kräfte in andere konventionelle Streitkräfte bzw. die Qualität der Kooperation mit diesen eine Rolle. Je mehr Hierarchieebenen und Behördengrenzen überwunden werden müssen, desto komplexer und vor allem langsamer werden OMCO. Allerdings gibt es hierzu nur wenig Forschung.

Grafik 3

Typen von OMCO

geordnet nach aufsteigender Komplexität, Invasivität und Intensität

wenig viel

Operation	Ursprung	Umfang	Dauer	Effektarten	Ort des Effekts	Art der Ziele
Operation Orchard 2007	**Israel** erstklassige Cyber-Macht mit ca. 5 000 Hackern	gezielter Angriff auf syrische Luftabwehr	wenige Stunden	ISR; Dienstblockade (DoS)	Fremdes Militärnetzwerk	Militärisches Ziel (Radar)
Irak 2007	**USA** erstklassige Cyber-Macht mit ca. 6 000 Hackern	breiter Angriff (Hunderte PCs)	Jahre	ISR; InfoOps/PsyOps; DoS	Fremde Netzwerke von Aufständischen	Zivile und militärisch genutzte Systeme
Glowing Symphony 2016 ff	**USA** erstklassige Cyber-Macht mit ca. 6 000 Hackern	sehr breiter Angriff (Hunderte Smartphones, PCs, Server)	Jahre	ISR; InfoOps/PsyOps; DoS; Sabotage (Löschung von Daten)	Fremde Netzwerke und Systeme in 35 Ländern	Zivile und militärisch genutzte Systeme
Georgien 2008	**Russland** erstklassige Cyber-Macht	breiter Angriff (Hunderte PCs)	Wochen	ISR; InfoOps; DoS	Fremde Netzwerke in Georgien	Zivile und militärisch genutzte Systeme
Ukraine 2014 ff	**Russland** erstklassige Cyber-Macht	sehr breiter Angriff (Hunderte Smartphones, PCs, Server), teils willkürliche, uneingeschränkte Zielauswahl	Jahre (andauernd)	ISR; InfoOps/PsyOps; DoS; Sabotage (Datenlöschung & kinetisch)	Fremde Netzwerke in der Ukraine, globale Kollateralschäden (Not Petya)	Zivile und militärische Ziele; kritische Infrastrukturen
Nitro Zeus 2016	**USA** erstklassige Cyber-Macht mit ca. 6 000 Hackern	sehr breiter Angriff (Hunderte Smartphones, PCs, Server), teils willkürliche, uneingeschränkte Zielauswahl	?	DoS; Sabotage (kinetisch)	Fremde Netzwerke im Iran	Zivile und militärische Ziele; kritische Infrastrukturen

DDoS Distributed Denial of Service (Gestreute Dienstblockade)
DoS Denial of Service (Dienstblockade)
IED Improvised Explosive Device (Unkonventionelle Sprengvorrichtung)
InfoOps Informations-Operationen
ISP Internet Service Provider
ISR Intelligence, Surveillance and Reconnaissance (Nachrichtengewinnung und Aufklärung)
OMCO Offensive militärische Cyber-Operation (in fremden Netzen)
PsyOps Psychologische Kriegsführung

Grafik 3 (Forts.)

Typen von OMCO (Forts.)

geordnet nach aufsteigender Komplexität, Invasivität und Intensität

wenig viel

Operation	Zeitpunkt der OMCO	Art der OMCO	Angriffs-komplexität der OMCO	Modus Operandi	Ziele der OMCO
Operation Orchard 2007	Erstschlag in Konfliktsituation	operativ	mittel	Malware	Deaktivieren der Luftabwehr als Enabler für konventionelle Operation
Irak 2007	In einem bewaffneten Konflikt	operativ und taktisch	gering bis mittel	ISP-Hijacking; Malware	Fallen stellen; Aufständische identifizieren; IEDs deaktivieren; Informationsgewinnung
Glowing Symphony 2016 ff	In einem bewaffneten Konflikt	operativ und taktisch	mittel bis hoch	Malware; Identitätsdiebstahl	Verlangsamen und Stören von ISIS-Kommunikationsnetzwerken und Social-Media-Aktivitäten; Informationsgewinnung
Georgien 2008	In einem bewaffneten Konflikt	operativ	gering	DDoS-Angriffe; Website-Veränderung (Defacement); Nutzung von Cyber-Söldnern	Störung der georgischen Kommunikation; Verwirrung stiften; Unterstützung konventioneller Truppen
Ukraine 2014 ff	In einem bewaffneten Konflikt	strategisch, operativ und taktisch	mittel bis hoch	DDoS-Angriffe; Website-Defacement; Nutzung von Cyber-Söldnern; Malware; Phishing; 0-Day-Schwachstellen	Ergänzung zu einer hybriden Full-Spectrum-Operation*; Unterstützung von Truppen im Feld; psychologische Effekte wie Induzieren von Angst und Unsicherheit
Nitro Zeus 2016	Erstschlag in Friedenszeiten	strategisch	sehr hoch	Malware; Multiple 0-Day-Schwachstellen	Irans Verteidigungsfähigkeit vermindern; Ausüben von politischem Zwang, um das Atomprogramm zu beenden

* Als Full-Spektrum-Strategie wird ein militärisches Vorgehen gegen alle Lebensbereiche des Gegners (gesellschaftlich, wirtschaftlich, militärisch) bezeichnet.

Sinnvolle Einsatzszenarien für offensive Bundeswehr-Cyber-Operationen

Wie gesehen eignen sich OMCO für bestimmte militärische Aufgaben und für andere nicht. Insofern wird im nächsten Schritt geprüft, welche der traditionellen Aufgaben der Bundeswehr OMCO abdecken oder ergänzen können.

Die Bundeswehr hat seit dem Ende des Kalten Krieges einen konzeptionellen Wandel von einer Armee zur Bündnis- und Landesverteidigung hin zu einer Armee in Auslandseinsätzen durchlaufen. Internationaler Terrorismus, Staatszerfall, organisierte Kriminalität, Migrationsbewegungen oder die Proliferation von Massenvernichtungswaffen galten seit Ende der 1990er Jahre als dominante Bedrohung.[78] Daher waren Krisenvorsorge und Krisenmanagement (inklusive Krisenprävention, Stabilisierung und Krisennachsorge) der vorwiegende Zweck von Auslandseinsätzen. Bedrohungen in der Form konventioneller Angriffe durch staatliche Akteure galten als eher unwahrscheinlich. Allerdings hat sich die Bedrohungswahrnehmung aufgrund der veränderten sicherheitspolitischen Lage in Europa durch die russische Aggression im postsowjetischen Raum verändert. Im *Weißbuch* von 2016 werden Krisenmanagement bzw. Peacekeeping und Landesverteidigung daher gleichrangig behandelt.[79] Den aktuellen Planungen zufolge soll »die Leistungsfähigkeit der Streitkräfte bis zum Jahr 2032 wieder prioritär an der Landes- und Bündnisverteidigung, der Bereitschaft zur Abschreckung und damit an den Verteidigungsplanungen der Nato ausgerichtet werden«.[80] Daneben werden in den *Verteidigungspolitischen Richtlinien* 2011 die folgenden Aufgaben definiert:

- Landesverteidigung als Bündnisverteidigung im Rahmen der Nordatlantischen Allianz;
- internationale Konfliktverhütung und Krisenbewältigung — darin eingeschlossen der Kampf gegen den internationalen Terrorismus;
- Beteiligung an militärischen Aufgaben im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik der EU;
- Beiträge zum Heimatschutz, das heißt Verteidigungsaufgaben auf deutschem Hoheitsgebiet, sowie Amtshilfe in Fällen von Naturkatastrophen und schweren Unglücksfällen, zum Schutz kritischer Infrastruktur und bei innerem Notstand;
- Rettung und Evakuierung sowie Geiselbefreiung im Ausland;
- Partnerschaft und Kooperation im Rahmen einer multinationalen Integration und globalen Sicherheitszusammenarbeit auf der ideellen Grundlage einer modernen Verteidigungsdiplomatie;
- humanitäre Hilfe im Ausland.[81]

Untersucht man die Einsätze der Bundeswehr empirisch, dann stellt sich für die Vergangenheit eine leicht andere Prioritätensetzung dar. Für die Analyse wurden die mehr als 50 Einsätze seit 1990 nach Kerndaten wie Einsatzdauer, verwendetem Personal und militärischem Gerät, Einsatzbeschreibung bzw. Mandatsaufgaben sowie nach den durchgeführten Funktionen der Bundeswehr ausgewertet.[82] Dabei wurde

78 BMVg, *Verteidigungspolitische Richtlinien* [wie Fn. 21].

79 Bundesregierung, *Weißbuch* [wie Fn. 1].

80 Rainer Glatz u.a., *Die Auslandseinsätze der Bundeswehr im Wandel*, Berlin: Stiftung Wissenschaft und Politik, Mai 2018 (SWP-Studie 7/2018), <www.swp-berlin.org/fileadmin/contents/products/studien/2018S07_kim_EtAl.pdf>.

81 BMVg, *Verteidigungspolitische Richtlinien* [wie Fn. 21], S. 12.

82 Gegen die Erkenntnisse der Analyse lässt sich natürlich ein gravierender Einwand vorbringen, nämlich dass sie nur

Tabelle 1

Von der Bundeswehr wahrgenommene Aufgaben in den Einsätzen seit 1990

Wahrgenommene Mandatsaufgaben	*Beispiele*	*Anzahl*
Verteidigung und Sicherung	Luftraumsicherung in Bosnien-Herzegowina (Deny Flight 1992), Schutz von Gebäuden in Afghanistan (Resolute Support 2015), maritimer Geleitschutz im Mittelmeer (Active Endeavor 2001), Schutz von Zivilisten oder Militärbeobachtern in Nordmazedonien (EXFOR 1998)	18
Logistik	Transporteinsätze, etwa Luftbrücken in Somalia (UNOSOM II 1993), Luftbetankung (AFISMA 2013), Transport von Personal und Material (SFOR 1996)	18
Aufklärung	Überwachungsflüge mit AWACS (Deny Flight 1992), mit Tornados (UNPROFOR 1995), Seeaufklärung der Marine (Enduring Freedom 2001), Panzeraufklärung und Gebirgsjägereinsatz an Land in Bosnien-Herzegowina (SFOR I+II 1996)	18
Ausbildung und Beratung	Ausbildung von Sicherheitskräften in Afghanistan (ISAF 2001), von Führungskräften (EUTM Somalia 2010), Einsatz von Pionieren und Sanitätern (EUTM 4Mali 2013), Ertüchtigung und Schulung im Waffeneinsatz (Irak 2014)	14
Verbindungswesen und Kommandostrukturen	Mitarbeit in Kommandostrukturen durch Stabsoffiziere vor Ort in der DR Kongo (Operation Artemis 2003) sowie Leitung von Einsätzen (ISAF 2001).	11
Militärbeobachter	United Nations Mission in Ethiopia and Eritrea (UNMEE 2004)	10
Medizinische Versorgung	United Nations Advance Mission in Cambodia (UNAMIC 1991)	8
Evakuierung	Operation Artemis (2003)	5
Kampfeinsatz	Teilnahme von Aufklärungs-Tornados an Luft-Boden-Angriffen im ehemaligen Jugoslawien (Allied Force 1999) oder aktuell in Syrien, Einsatz in Afghanistan (Enduring Freedom & ISAF 2001), Bekämpfung von Piraterie in Somalia (Operation Atalanta 2008).	4
Entwaffnung	EUFOR Concordia in Nordmazedonien (2003)	3
Versorgung	Albania Force (AFOR 1999)	2

gezählt, welche Funktion bzw. militärische Komponente im jeweiligen Einsatz zur Verwendung kam (siehe Tabelle 1). Die von der Bundeswehr wahrgenommenen Mandatsaufgaben wurden der Website des BMVg entnommen. Wenn die Bundeswehr mehrere Funktionen im gleichen Einsatz ausgeübt hat, wurden diese entsprechend mehrfach gezählt.

Insgesamt zeigt sich also, dass die Bundeswehr nach 1990 ein defensives Aufgabenspektrum erfüllt hat. Die Einsätze sind gekennzeichnet vom Ziel der Konfliktverhütung und Krisenbewältigung im Rahmen multilateraler Mandate (EU-GSVP, Nato, UN).

vergangene Einsätze der Bundeswehr einschließt, die nicht notwendigerweise Aussagen über die Zukunft zulassen. Wenn die Bundeswehr wieder die Aufgabe der Landesverteidigung stärker in den Blick nimmt, könnten strategische Cyber-Angriffe im Verteidigungsfall vermehrt in den Fokus rücken. Auch ist mit einer zunehmenden Digitalisierung der meisten Länder und somit weiteren Anwendungsfällen zu rechnen.

Dieser Fokus ist auch bei den zahlreichen Unterstützungsleistungen im Bereich von Transport und Logistik, der Aufklärung von Zielen, der Erstellung von Lagebildern und des Schutzes von Personal und Objekten bestimmend. Die Bundeswehr ist in der Regel also nur indirekt an Kampfhandlungen beteiligt, indem sie Lagebilder weitergibt, die von den Alliierten dann wiederum zur Bekämpfung konkreter Ziele verwendet werden. Die Ausnahme hiervon ist der Afghanistaneinsatz, der als konventioneller Kampfeinsatz zu werten ist. Betrachtet man die geografische Verteilung der Einsätze der letzten 30 Jahre, so fanden diese vorwiegend in wenig entwickelten und wenig digitalisierten Regionen mit schwacher Staatlichkeit statt. Die Opponenten bestanden ganz überwiegend aus gering technisierten Rebellengruppen bzw. Aufständischen.

Vergleicht man das Spektrum denkbarer militärischer Cyber-Operationen mit dem bisherigen Einsatzprofil der Bundeswehr, so zeigt sich nur eine begrenzte Überschneidung.

Vergleicht man das zuvor analysierte Spektrum militärischer Cyber-Operationen mit dem Einsatz- und Aufgabenprofil der Bundeswehr, so zeigt sich nur eine begrenzte Überschneidung. Für das spezifische Aufgabenprofil der Bundeswehr scheinen OMCO des Typs ISR, InfoOps und begrenzte Denial-of-Service-Angriffe in operativen Kontexten sinnvoller zu sein als zum Beispiel strategische Angriffe auf zivile kritische Infrastrukturen in Friedenszeiten. Ungeeignet sind OMCO indes überall dort, wo eine physische Präsenz von Soldatinnen und Soldaten erforderlich ist, etwa bei der Räumung von konventionellen Minen, beim Objektschutz, bei Logistik- und Transportmissionen, bei medizinischer Versorgung, bei Ausbildungs- und Beratungsmissionen, der ABC-Abwehr, im militärischen Verbindungswesen sowie bei Militärbeobachtermissionen. Auch bei humanitärer Hilfe dürfte die Anwesenheit menschlicher Kräfte sinnvoller sein als das Einsetzen von OMCO.

ISR-Operationen

Die Fallstudien haben gezeigt, dass OMCO vom Typ ISR in fast allen Fällen eine herausragende Rolle gespielt haben, weil damit wichtige militärische Informationen gewonnen werden konnten. ISR-OMCO passen in das defensive Aufgabenprofil der Bundeswehr, die zum Beispiel in der Vergangenheit immer wieder zahlreiche Aufklärungsfunktionen, ob zu Land, Luft oder zur See, wahrgenommen hat. Da immer mehr militärische Systeme digitalisiert, vernetzt und automatisiert werden, ist ISR bzw. Cyber-Spionage für zahlreiche Staaten eine gewinnbringende und relativ risikoarme Option. Durch eine ISR-OMCO in gegnerischen militärischen Hauptquartieren, Kommunikations- oder Logistiknetzwerken können taktische und operative Informationen über gegnerische Luft-, See- und Landbewegungen und Truppenpositionen gesammelt werden. Die Agent-X-Malware, die ukrainische Artilleriestellungen enttarnt hat, aber auch die Ortsbestimmung (Triangulation) feindlicher Kämpfer mittels Handy-Geopositionsdaten in dünnbesiedelten Regionen (Afghanistan-Hack des KdoCIR 2015) sind Beispiele dafür.[83]

Weiträumige Gebiete wie Mali, der Kongo, Somalia oder Afghanistan, wo die Bundeswehr aktiv war und ist, kommen für diese spezielle Art des ISR eher in Frage als urbane Gebiete, wo zahlreiche Mobiltelefone die Erkennungsrate verschlechtern, da einzelne Telefone in der Masse verschwinden (»signal to noise ratio«). Allerdings darf der Digitalisierungsgrad einer Einsatzregion auch nicht zu gering sein, denn dann sind OMCO nutzlos. Bei der Nutzung von ISR für Landaufklärung gelten die territorialen Einschränkungen, die bei taktischen OMCO identifiziert wurden, etwa die Störanfälligkeit von elektronischem Equipment und Reichweitenbegrenzungen. Zudem stellen sich bei Cyber-Angriffen gegen Internet-Service-Provider in anderen Ländern rechtliche Fragen, insbesondere wenn Bundeswehrsoldaten im Rahmen eines Peacekeeping-Mandats auf die explizite Einladung einer Regierung angewiesen sind.

Bei anderen Operationsarten ergeben sich ähnliche Hürden und Herausforderungen, etwa bei der Seeaufklärung oder gar der Pirateriebekämpfung. Um in diesem Bereich relevante ISR zu generieren, müssten Informationen über Schiffsbewegungen erlangt werden. Das kann auf verschiedenen, teils risikobehafteten Wegen geschehen: entweder via OMCO gegen Schiffe selbst (Betriebssysteme, industrielle Steuerungscontroller zum Beispiel in Maschinen), via Cyber-Angriffe auf Logistiksysteme von Häfen, via Cyber-Spio-

83 Matthias Gebauer, »Bundeswehr-Hacker knackten afghanisches Mobilfunknetz«, *Spiegel online*, 23.9.2016, <www.spiegel.de/politik/ausland/cyber-einheit-bundeswehr-hackte-afghanisches-mobilfunknetz-a-1113560.html>.

nage in Reedereien und somit gegen Firmen anderer Länder oder gar gegen kollektiv genutzte Systeme wie GPS-Navigation oder das Global Maritime Distress and Safety System.[84] Funkverbindungen und Kommunikationsschnittstellen mit der Außenwelt sind immer auch eine Angriffsfläche für Cyber-Attacken. Angriffe gegen kollektiv genutzte Systeme wie GPS bergen allerdings enorme Risiken für unbeabsichtigte Kollateralschäden, während gezieltere ISR-Angriffe auf einzelne Schiffe zumindest theoretisch weniger risikobehaftet sind. Erstere sollten tunlichst vermieden werden. Cyber-Operationen gegen Hochseeschiffe oder die zivilen Reedereien anderer Länder könnten internationale Verwerfungen produzieren und im schlimmsten Fall Häfen und somit die Seeschifffahrt lahmlegen (so geschehen bei *Not-Petya*). Mobilfunktriangulation gegen Piraten scheint aufgrund der Reichweite von Mobilfunk auf hoher See nur begrenzt sinnvoll zu sein. Ferner gilt etwa Somalia als eines der am wenigsten digitalisierten Länder der Welt, so dass dort der Nutzen von ISR aller Erkenntnis nach gering ist.

Die Fallstudien haben zudem gezeigt, dass die Landaufklärung, etwa von gegnerischer Infanterie oder Panzerverbänden, mit digitalen Mitteln begrenzt effizient sein dürfte. Digitalisierte Infanteristen der Zukunft sind verwundbarer gegenüber taktischer ISR als Infanterie mit wenig digitalem Equipment. Viele Armeen gehen aus Angst vor Spionage und Hacking dazu über, den Einsatz digitaler Geräte wie Smartphones zu reglementieren und einzuschränken. Statt aufwendig Tausende Smartphones von Soldaten und Soldatinnen zu hacken, dürfte es in den meisten Fällen effektiver, simpler und kostengünstiger sein, elektronisches Equipment mittels traditioneller elektronischer Kampfführung lahmzulegen.

Alternativ könnten sich ISR-OMCO gegen gegnerische militärische Kommando- und Befehlsinfrastrukturen richten, etwa Einsatzführungskommandos oder Fernmeldeeinheiten. Eine solche ISR-Operation dürfte indes in hohem Maße technisch und operativ komplex und nicht einfach durchzuführen sein. Am Ende steht hier immer eine Kosten-Nutzen-Abwägung: Ist es den Aufwand wert, kostspielig in gegnerische Hauptquartiere zu hacken, oder kann man Aufklärung nicht mit traditionellen und weniger invasiven Mitteln wie Aufklärungssatelliten oder Drohnen durchführen?

Der Einsatz moderner digitaler Kommunikationsstrategien wäre in Missionen zur humanitären Versorgung generell sinnvoll.

InfoOps

Diese Erwägungen führen zur zweiten sinnvollen OMCO-Verwendung: InfoOps könnten bei den meisten Bundeswehrmissionen eine begleitende Rolle spielen. Solche Operationen würden aber nach gängiger Praxis vermutlich nur das Verbreiten von wahren Informationen und nicht die negative Subversion und Desinformation nach russischem Vorbild umfassen. Es ist denkbar, dass Social-Media-Teams der Bundeswehr zum Beispiel Online-Werbung schalten, um die Zielbevölkerung zu informieren oder positiv zu beeinflussen. Bei der Repatriierung von Geflüchteten können InfoOps bedingt zweckmäßig sein, etwa um zielgenau Informationen an die betreffenden Personen zu übermitteln. Auch bei Evakuierungsaufgaben könnten InfoOps durchgeführt werden, zum Beispiel indem Nachrichten auf die Smartphones jener Individuen, die es zu evakuieren gilt, aufgespielt werden oder indem diese sogar per Telefon geortet werden. Bei deutschen Staatsbürgern im Ausland stellen sich hierbei aber rechtliche Fragen wegen des damit verbundenen Eingriffs in Grundrechte. Auch das gezielte Senden von Nachrichten auf Handys in Zielregionen, nach dem Vorbild der NSA-Operation im Irak 2007, kann, je nach Missionsauftrag, hilfreich sein. Der Einsatz moderner digitaler Kommunikationsstrategien wäre in Missionen zur humanitären Versorgung generell sinnvoll. Das gilt auch für das Informieren über Entwaffnungsstützpunkte in der Krisennachsorge. Dabei würde es sich jedoch um keine genuinen offensiven Cyber-Fähigkeiten handeln, sondern lediglich um modernere digitale Kommunikationsformen.

Wie genau eine offensivere Bekämpfung von digitaler Propaganda aussehen könnte, hat die Operation *Glowing Symphony* gezeigt. Wenn eine solche Operation aber im globalen Maßstab stattfinden würde, müsste dies im Bundestagsmandat dargelegt sein und

84 Patrick Tuckler, »Hacker Shows How to Break Into Military Communications. Design Flaws in Communication Equipment Could Affect Aircraft and Troop Communication Equipment«, *Defense One* (online), 7.8.2014, <https://www.defenseone.com/technology/2014/08/hacker-shows-how-break-military-communications/90947/> (Zugriff am 21.4.2020).

wären zuvor einige rechtliche Fragen zu klären. Für die US-CYBERCOM gestaltet sich das Entfernen von Online-Propaganda auf Servern von US-Firmen wie *Facebook* weniger komplex als etwa für die Bundeswehr, da sich die Firmen unter US-Jurisdiktion befinden. Dass Online-Propaganda auf kommerziellen Diensten anderer Länder gehostet wird, scheint eher die Norm als die Ausnahme zu sein. Da Desinformation, Propaganda und Hate-Speech auch ein Problem der Rechtsdurchsetzung ist, sollten hierzu wohl eher zivile Konsultations- bzw. Strafverfolgungsmechanismen (»Notice-and-Take-down-Prozesse«) mit anderen Ländern genutzt werden, bevor die Bundeswehr eine Cyber-Operation startet. Denkbar sind indes aber gezielte Maßnahmen wie Phishing-E-Mails, die an einzelne Propaganda-Accounts gesendet werden, um diese zu übernehmen, ohne die Plattform als Ganzes zu stören.

Begrenzte DoS-OMCO zur Begleitung von Kampfeinsätzen

Der dritte Nutzen vom OMCO besteht in der begrenzten taktischen bzw. operativen Begleitung von Kampfeinsätzen. Die analysierten offensiven Cyber-Operationen ereigneten sich überwiegend im Kontext von Kampfeinsätzen in bewaffneten Konflikten. Genuine Kampfeinsätze machen zwar nur einen kleinen Teil aller Out-of-area-Einsätze der Bundeswehr aus (Allied Force 1999, ISAF 2001, MINUSMA 2013, Counter Daesh 2015), es sind aber zugleich die herausforderndsten Einsätze.

Operation *Glowing Symphony* und die NSA-Operation im Irak 2007 haben gezeigt, wie begrenzt der Nutzen von taktischen OMCO zur Einsatzunterstützung von Landstreitkräften und auch Spezialkräften ist. Es ist zum Beispiel denkbar, dass das Kommando Spezialkräfte in einer taktischen OMCO eine Schadsoftware in gegnerischen Stützpunkten hinterlässt oder gegnerische Computer konfisziert, die dann forensisch ausgewertet werden.

Ein Cyber-Angriff auf gegnerische Luftabwehrstellungen oder zur Zerstörung von Radaranlagen wäre für die Bundeswehr vermutlich ein sinnvolles Einsatzszenario.

Operation *Orchard* ist ein Beleg dafür, dass Cyber-Fähigkeiten, die DoS- oder Sabotage-Effekte zeitigen, unter bestimmten Umständen für die Luftraumsicherung genutzt werden können, nämlich dann, wenn gegnerische Radarsysteme, Boden-Luft-Raketen oder gar digitale Komponenten von Kampfflugzeugen gehackt und gestört werden. Lufteinsätze sind bei Bundeswehrmissionen keine Seltenheit. Insofern wäre ein Cyber-Angriff auf gegnerische Luftabwehrstellungen oder zur Zerstörung von Radaranlagen vermutlich ein sinnvolles Einsatzszenario. Dieser Plan wird aber nicht bei jedem Gegnertyp funktionieren. Generell erfordern solche OMCO einen hohen logistischen und nachrichtendienstlichen Aufwand, um komplex geschützte gegnerische Militärsysteme zu hacken. Damit verbunden ist stets eine gewisse Unsicherheit über die tatsächliche Wirkung. Aufgrund der Resilienzproblematik kann es für militärische Entscheider in vielen Fällen sinnvoller sein, statt auf aufwendige und unzuverlässige Cyber-Angriffe gegen militärische Ziele zu setzen, diese Ziele lieber kinetisch auszuschalten.

Szenario: Verteidigungsfall

Die Bundeswehr war bisher glücklicherweise noch nie tatsächlich mit einer Situation der Landesverteidigung konfrontiert. Für OMCO, die akut dem Schutz des eigenen Landes dienen, gibt es keine empirischen Beispiele, so dass diese Variante nur mittels eines Szenarios und hypothetischer Annahmen beschrieben werden kann. Strategische Cyber-Angriffe gegen Deutschland ohne konventionelle Komponente sind zwar denkbar, aber aufgrund ihrer hohen Kosten, operativen Komplexität und schwer zu beherrschenden strategischen Effekte eher unwahrscheinlich.[85] Ein strategischer Cyber-Angriff nach dem Vorbild der Operation *Nitro Zeus* gegen den Iran 2016 würde sich vermutlich zu einem Nato-Verteidigungsfall zuspitzen und nach aktueller Nato-Doktrin auch mit konventionellen Mitteln beantwortet werden können.[86] Daraus könnte sich eine Eskalationsspirale ergeben, in der Nato-Staaten und potentieller Angreifer sich mittels strategischer OMCO gegenseitig ihre zivilen und militärischen Infrastrukturen ausschalten und auf beiden Seiten das gesellschaftliche und wirtschaft-

85 BMVg, *Bericht zum Themenkomplex Cyber-Verteidigung* [wie Fn. 22], S. 33.

86 Jens Stoltenberg, »NATO Will Defend Itself«, Brüssel: Nato, 27.8.2019, <www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en>.

liche Leben massiv gestört wird. Das dürfte nicht im Interesse der Kontrahenten liegen, so dass einige Politikwissenschaftler theoretisieren, dass Staaten bei offensiven Cyber-Attacken zu Zurückhaltung neigen würden, um dieses Worst-case-Szenario zu vermeiden.[87] Am plausibelsten erscheint daher ein konventioneller Angriff, der eventuell von OMCO begleitet wird. Da oben gezeigt wurde, dass Cyber-Angriffe, die in der Frühphase von Konflikten platziert werden, am sinnvollsten sind, liegt die Annahme am nächsten, dass solche Attacken als Enabler für einen konventionellen Angriff auf europäisches Territorium genutzt würden.

Ein Ausfall von GPS oder des Internets hätte weltweit Folgen für den Personen- und Warenverkehr und das Finanzsystem, weshalb von Angriffen auf diese Infrastrukturen dringend abzuraten ist.

Wie könnte das Kommando Cyber- und Informationsraum (KdoCIR) darauf reagieren? Vom KdoCIR lancierte OMCO könnten sich a) gegen gegnerische militärische Befehls- und Kommandostrukturen richten, um die Kommunikation zwischen vorrückenden Streitkräften zu behindern und zu verlangsamen (DoS); sie könnten sich b) gegen die Software gegnerischer Waffensysteme wie Panzer, Flugzeuge bzw. Drohnen oder die digitale Infanterieausrüstung richten, um diese lahmzulegen; sie könnten sich c) gegen gegnerische Cyber-Kommandos und CNO-Einheiten richten, um deren Fähigkeiten zu binden (»digitaler Gegenangriff« bzw. »Hackback«).[88] Das Völkerrecht gestattet zudem in einem Krieg auch d) Angriffe gegen zivile Infrastrukturen, so sie denn für militärische Zwecke verwendet werden. So wie in einem kinetischen Konflikt Brücken gesprengt werden können, um ein gegnerisches Vorrücken zu verlangsamen, können digitalisierte Logistik- und Verlegungssysteme gestört werden, um die Dislozierung großer Truppenkontingente zu verlangsamen. Zum Beispiel könnten öffentliche Infrastrukturen wie GPS-Satelliten gehackt werden, um Drohnen zu verwirren.[89] Allerdings gehen von solchen breiten, wenig restriktiven Angriffen enorme und schwer antizipierbare Kollateralrisiken aus.[90] Ein Ausfall von GPS oder des Internets hätte weltweite Implikationen für den Personen- und Warenverkehr und das Finanzsystem, weshalb von Angriffen auf diese Infrastrukturen dringend abzuraten ist. Gezielte OMCO gegen einzelne digitalisierte Waffensysteme wären mit weniger Risiken behaftet, da hier ungewollte Kollateraleffekte zumindest theoretisch besser eingegrenzt werden könnten. Gerade weil moderne digitalisierte Waffensysteme so viele IT-Schwachstellen bergen, können OMCO zur Landesverteidigung sinnvoll sein. Da konventionelle Offensiven mit enormem logistischem Aufwand einhergehen, also eine hohe operative Komplexität haben, dürften sie besonders störanfällig für DoS-OMCO sein.

Wegen des oben beschriebenen Kaltstartproblems erfordern OMCO gegen militärisches Gerät eine Phase der Vorbereitung, um im Verteidigungsfall wirksam zu sein. Damit Schwachstellen im Softwarecode gegnerischer Kampfflugzeuge identifiziert werden können, müsste eine Kopie des Codes mittels Cyber-Spionage von den Herstellerfirmen entwendet werden. Die USA werfen China genau diese Art der vorbereitenden Industriespionage im Fall des F-35-Kampfjets vor.[91] Zur »Vorbereitung des Schlachtfelds« (»preparation of the battlefield«) werden daher bereits in vielen Staaten in Friedenszeiten Listen mit potentiellen Angriffszielen gepflegt, gegnerische IT-Systeme kartografiert und auf Softwareschwachstellen hin geprüft, um (nach dem Vorbild der NSA »Treasure Map«) im Konfliktfall schneller einsatzbereit zu sein. Mit dieser Erstellung aktueller Cyber-Lagebilder geht ein erheblicher Kosten- und Ressourcenaufwand einher. Auch birgt die dahinterstehende Logik präemptiver Cyber-Angriffe ein enormes Konfliktverschärfungspotential. Staaten sind bei Angriffen auf kritische Infrastrukturen eher bereit zu digitalen Gegenschlägen, was für ein gewisses Eskalationsrisiko spricht. Noch bevor OMCO eingesetzt werden, wird dadurch eine Aufrüstungsdynamik befeuert und sinkt die globale Sicherheit des Cyber- und Informationsraums. Bei

87 Valeriano/Maness, *Cyber War versus Cyber Realities* [wie Fn. 46], S. 226ff.

88 Reinhold/Schulze, *Digitale Gegenangriffe* [wie Fn. 10].

89 Adam Rawnsley, »Iran's Alleged Drone Hack: Tough, but Possible«, *Wired* (online), 16.12.2011, <www.wired.com/2011/12/iran-drone-hack-gps/> (Zugriff am 5.5.2020).

90 Brian Barret, »The Air Force Will Let Hackers Try to Hijack an Orbiting Satellite«, *Wired* (online), 17.9.2019, <www.wired.com/story/air-force-defcon-satellite-hacking/> (Zugriff am 21.4.2020).

91 Franz-Stefan Gady, »New Snowden Documents Reveal Chinese behind F-35 Hack«, *The Diplomat* (online), 27.1.2015, <https://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/> (Zugriff am 7.5.2020).

diesem Trend haben hochdigitalisierte Staaten mehr zu verlieren als zu gewinnen. Für das KdoCIR stellt sich damit ein Dilemma: OMCO, die eigentlich allein der Landesverteidigung dienen sollen, müssen, um effektiv zu sein und das Kaltstartproblem zu umgehen, eine offensive Komponente in Friedenszeiten beinhalten. Ob dies legal ist und dem Ziel der Friedenssicherung dienlich ist, ist unklar.

Ergebnisse und Ausblick

Es zeigt sich, dass OMCO für die Bundeswehr nur in begrenztem Umfang geeignet sein dürften. Die sinnvollen Verwendungszwecke konzentrieren sich auf ISR, also auf militärische Spionagetätigkeiten, gezielte, das heißt taktische Informationsoperationen zur Begleitung von konventionellen Out-of-area-Einsätzen und auf ganz spezifische Fälle von DoS-Operationen gegen gegnerische Waffensysteme, etwa bei Kampfeinsätzen oder im Kontext der Landesverteidigung. Die Bundeswehr sollte diese OMCO aber tendenziell sehr restriktiv handhaben, das heißt gegen sehr wenige Ziele richten, von denen zudem nur ein geringes Risiko für weltweite Kollateralschäden ausgeht. Eine sorgfältige Folgenabschätzung im Vorfeld und eine umfassende parlamentarische Kontrolle sind daher dringend geboten. Die bisherige Praxis der Geheimhaltung rund um offensive Cyber-Operationen ist problematisch. Langfristig ist damit ein Trend der »Vernachrichtendienstlichung« von militärischen Einsätzen zu befürchten. Es besteht das Risiko, dass Bundeswehr-OMCO, ähnlich wie nachrichtendienstliche Cyber-Spionage, als grundsätzlich geheimhaltungswürdig eingestuft und so die Möglichkeiten der Kontrolle durch den Verteidigungsausschuss reduziert werden.[92] Eine solche Entwicklung sollte vermieden werden.

Zudem finden zahlreiche Bundeswehroperationen in wenig digitalisierten Regionen statt. Die Gegner in diesen Räumen, wie Rebellen, Piraten oder Guerilla-Kräfte, sind kaum technisiert und häufig mit simplen AK-Sturmgewehren und nicht mit High-Tech-Equipment unterwegs. Cyber-Operationen gegen solche Akteure sind nur begrenzt sinnvoll. Allerdings ist mit zunehmender Digitalisierung davon auszugehen, dass der Nutzen von OMCO in naher Zukunft steigen könnte.

Es ist bemerkenswert, dass es in der Forschungsliteratur, in den strategischen Dokumenten der Bundeswehr bzw. in der politischen Debatte bisher kaum Überlegungen gibt, inwiefern Cyber-Operationen für die Krisenprävention, für Stabilisierungsaufgaben und die Krisennachsorge nützlich sein könnten. Hier gibt es erheblichen Forschungsbedarf. In der akademischen Diskussion ist das Thema komplett unterbelichtet. Ferner fehlt es diesbezüglich an empirischen Präzedenzfällen. Es wäre aber vielversprechend, über eine »Cyber im Krisenmanagement«-Strategie nachzudenken. Es sollten konkrete Ziele formuliert werden, was mit Cyber-Operationen im Krisenmanagement erreicht werden soll und kann. Die Ziele sollten operationalisierbar und evaluierbar sein. Im Themenkomplex »Cyber und Konfliktmanagement« könnte die Bundesregierung einen wichtigen Beitrag zur Entwicklung von Cyber-Doktrinen leisten, da Deutschland im Bereich der Krisenbearbeitung besonders aktiv ist und über historische Erfahrungen verfügt. Andere hochdigitalisierte Nationen sind bei der Konzipierung ihrer Cyber-Strategie auch noch nicht weiter, da sie andere Schwerpunkte verfolgen.

Deutschland sollte auch in Zukunft daran festhalten, keine strategischen OMCO zu planen und zu entwickeln. Die strategische Verwendung von OMCO erscheint operativ zu aufwendig, ist extrem risikobehaftet und zudem der globalen Sicherheit des Cyber- und Informationsraums unzuträglich. Außerdem ist mit der Planung strategischer OMCO ein enormer Ressourcenaufwand verbunden, den das überschaubare Personal von KdoCIR realistisch gesehen kaum wird leisten können. Das KdoCIR verfügt nur über wenige Hundert Hacker, hat daher also nur begrenzte Mittel, die allenfalls selektiv eingesetzt werden können. Eine strategische Nutzung von OMCO in Friedenszeiten dürfte im Übrigen auch wegen des defensiven Auftrags der Bundeswehr und der grundrechtlichen Implikationen ausscheiden.

Nichtsdestotrotz ist eine aktivere Diskussion über rechtliche Aspekte angebracht, die in der vorliegenden Studie nur marginal behandelt werden konnten. Es ist klar, dass Bundeswehr-OMCO rechtmäßig nur für die Verteidigung (GG Art. 87a), im Kontext multi-

92 Christian Marxsen, »Verfassungsrechtliche Regeln für Cyberoperationen der Bundeswehr Aktuelle Herausforderungen für Einsatzbegriff und Parlamentsvorbehalt«, in: *Juristen-Zeitung*, 72 (2017) 11, S. 543 – 552 (551).

lateraler Out-of-area-Einsätze (GG Art. 24) und in limitiertem Umfang im Rahmen der Amtshilfe (GG Art. 35) eingesetzt werden können. Allerdings gibt es aus Sicht von Verfassungs- und Völkerrechtlern hier erhebliche Grauzonen, die sich vor allem dadurch ergeben, dass die Eigenheiten von Cyber-Operationen mit 70 Jahre alten Verfassungsbegriffen nicht unzweideutig beschrieben werden können.[93] So hängt zum Beispiel die Frage der Parlamentsbeteiligung daran, welche Arten von Cyber-Operationen als eine »bewaffnete Unternehmung« bzw. als zu erwartender Einbezug in eine solche zu werten sind. Sind reine nichtdisruptive ISR-Operationen bereits eine bewaffnete Unternehmung im Cyber-Raum? Oder gilt dies erst für eher invasive Operationen nach dem Vorbild von *Orchard* oder gar *Nitro Zeus*? Umgekehrt ist zu fragen, ab wann bei hybriden Cyber-/Desinformationsoperationen, die unterhalb der völkerrechtlichen Schwelle eines bewaffneten Konflikts ablaufen, eine Verteidigungssituation erreicht wird, in der die Bundeswehr im »Informationskampf« aktiv werden darf. Cyber-Sicherheit, Gefahrenabwehr und auch aktive Cyber-Abwehr sind in Deutschland Sache des Bundesministeriums des Innern bzw. der Bundesländer.

Eine ungeklärte Frage ist auch die territoriale Reichweite von Bundeswehrmandaten vor dem Hintergrund der Grenzenlosigkeit des Cyber- und Informationsraums: Konventionelle Einsätze sind auf spezifische Regionen begrenzt. *Glowing Symphony* betraf zivile Ziele und Infrastrukturen in 35 Ländern weltweit. Schließlich ist zu klären, wie in Deutschland der rechtliche Status von präemptiven, vorbereitenden Praktiken in Friedenszeiten zu bewerten ist (»preparation of the battlefield«). Diese erfordern nämlich invasive Spionageaktivitäten in sensiblen gegnerischen Netzen. So etwas in Friedenszeiten durchzuführen bedeutet, die territoriale Integrität eines Gegners zu verletzen, was als unfreundlicher oder gar feindlicher Akt verstanden werden kann. Derartige Handlungen sind dem Ziel der Friedenssicherung und dem friedlichen Zusammenleben der Völker sicher nicht zuträglich.

93 Siehe zum Beispiel die Diskussion bei Ladiges, »Der Cyberraum« [wie Fn. 18], bei Bothe, *Stellungnahme zu Rechtsfragen des Cyberwar* [wie Fn. 8] oder bei Marxsen, »Verfassungsrechtliche Regeln« [wie Fn. 92].

Abkürzungen

ABC	Atomare, biologische und chemische (Kampfstoffe)
AFISMA	African-led International Support Mission to Mali
AFOR	Albania Force
APT	Advanced Persistent Threat
AWACS	Airborne Warning and Control System
BMVg	Bundesministerium der Verteidigung
BND	Bundesnachrichtendienst
CERTBw	Computer Emergency Response Team Bundeswehr
CIR	Cyber- und Informationsraum
CNE	Computer Network Exploitation
CNO	Computer Netzwerk Operationen
DDoS	Distributed Denial of Service
DoS	Denial of Service
EUTM	European Union Training Mission
EXFOR	Extraction Force
GASP	Gemeinsame Sicherheits- und Verteidigungspolitik
GG	Grundgesetz
InfoOp	Informationsoperation
IED	Improvised Explosive Device
InspCIR	Inspekteur des Cyber- und Informationsraums
ISAF	International Security Assistance Force (in Afghanistan)
ISR	Intelligence, Surveillance and Reconnaissance
KdoCIR	Kommando Cyber- und Informationsraum
MINUSMA	Mission multidimensionnelle intégrée des Nations Unies pour la stabilisation au Mali
NSA	National Security Agency
OMCO	Offensive militärische Cyber-Operation (in fremden Netzen)
OSINT	Open Source Intelligence
PsyOp	Psychologische Operation
SFOR	Stabilisation Force (in Bosnia and Hercegovina)
UNAMIC	United Nations Advance Mission in Cambodia
UNMEE	United Nations in Ethiopia and Eritrea
UNOSOM	United Nations Operations in Somalia
UNPROFOR	United Nations Protection Force
US CYBERCOM	United States Cyber Command

Weiterführende Literatur

Matthias Schulze
Überschätzte Cyber-Abschreckung.
Analyse der in der neuen US Cyber-Doktrin vorgesehenen Abschreckungspotenziale und Lehren für Deutschlands »aktive Cyberabwehr«
SWP-Aktuell 39/2019, Juli 2019, 8 Seiten

Matthias Schulze
»German Military Cyber Operations are in a Legal Gray Zone«
Lawfare Blog (online), 8.4.2020

Matthias Schulze
Governance von 0-Day-Schwachstellen in der deutschen Cyber-Sicherheitspolitik
SWP-Studie 10/2019, Mai 2019, 39 Seiten